LUISS

Department of
Political Sciences
Chair of Security Law and Constitutional Protection

Bulk Interceptions and Privacy Rights in Europe: the ECtHR Judgment *Big Brother Watch*

Prof. Davide Paris
SUPERVISOR

Prof. Francesco Cherubini
CO-SUPERVISOR

Edoardo Rega
Matr. 647202
CANDIDATE

Academic Year 2022/2023

Ai nonni Gigi e Guglielmo,

Ai miei genitori,

A chi c'è sempre stato

INDEX

INTRODUCTION

On the eve of June 5th 2013, *The Guardian*, a respected British newspaper, published an article entitled "*NSA collecting phone records of millions of Verizon customers daily*", throwing a spark destined to burst into flames. The article shed light on several gathering practices operated by the National Security Agency (NSA), the main American intelligence agency. The following days new articles were published, and the entire world was shocked by the discovery of an interconnected web of relations based on an incredible exploitation of mass surveillance and bulk interception techniques and subsequent transmission of the collected data to other countries' agencies within the most important secret services, including the already mentioned NSA and the British Government Communication Headquarters (GCHQ), aimed to prevent possible plots against democracies and their people. The man behind the revelations, as revealed a week after the Verizon article, was Edward Snowden, a former Central Intelligence Agency (CIA) contractor disillusioned from his work for the intelligence agency.

It is undeniable that Snowden's revelations fed the already existing debate on the balance between security and privacy rights: people started questioning about the proportionality of governments actions, which clearly limited one of the main unalienable human rights.

Article 8 of the European Convention on Human Rights (ECHR), which serves as the cornerstone of privacy protection within the European continent, states that "*Everyone has the right to respect for his private and family life, his home, and his correspondence*". This is a fundamental human right, and its significance in the digital era should not be underestimated as the latest technological developments could undermine its legacy. However, recent judicial rulings, most notably the groundbreaking decisions taken by the Grand Chamber of the European Court of Human Rights (ECtHR) in *Zakharov v. Russia*[1] and the watershed case of *Big Brother Watch and Others v. United Kingdom*[2], have ushered in a new era of jurisprudential inquiry. These pivotal judgments have catalyzed a reexamination of the delicate equilibrium between individual privacy and the imperatives of state security, shedding

[1] Case of *Zakharov v. Russia*, Judgment of the European Court of Human Rights, 2015.
[2] Case of *Big Brother Watch and Others v. The United Kingdom*, Judgment of the European Court of Human Rights, 202.

light on the fundamental question of how to strike the right balance in an era defined by rapid technological advancements and evolving security concerns.

This thesis will embark on an exploration of the right to privacy in Europe, delving into its historical roots and its contemporary challenges and issues, trying to understand what the future trajectories of the legal framework revolving around this right could be. In the light of this, the main aim of the thesis will be to identify whether the European Court of Human Rights, dealing with the bulk interceptions techniques, as useful as invasive, has succeeded in protecting the right to privacy or not through its latest rulings. The work is aimed to answer the following questions: did the ECtHR, in particular in the case *Big Brother Watch*, strike a fair balance between security and the right to privacy, or did it accept a too intrusive restriction of the right to privacy to secure that the States can continue to carry out bulk interceptions?

In order to reach the final objective, this thesis will be divided into three distinctive chapters, each trying to offer a perspective on the right to privacy in Europe and its evolution in the 21st century.

Chapter one initiates the exploration by delving into the critical theme of balancing security and privacy in the lives of European citizens: principles of proportionality, consent, and accountability will be brought in the foreground in order to provide a comprehensive overview of the dichotomy security-privacy rights. Within this chapter, a series of national provisions pertaining to privacy, scrutinizing their efficacy and compatibility with the overarching principles of the ECHR will be dissected: starting from the nearest Italian example, the legal frameworks of three other countries as France, Germany, and the United Kingdom will be examined trying to scrutinize their compliance with the latest European standards.

As the European Convention of Human Rights is not the only legislative source within the European boarders which regulates the right to privacy, a paragraph of this first chapter will be dedicated to other European sources of law: the latest European Directives and articles 7 and 8 of the European Union Charter of Fundamental Rights will be closely analyzed, culminating in a brief examination of the *Digital Rights Ireland Ltd v. Minister for Communication et al and Kärtner Landesregierung*[3] case, a

[3] Case of *Digital Rights Ireland Ltd v. Minister for Communication et al and Kärtner Landesregierung*, Judgment of the European Court of Justice, 2014

seminal ruling concerning privacy rights of the European citizens by the Court of Justice of the European Union.

The analytical journey will come to a crescendo with an exhaustive scrutiny of the European Court of Human Rights perspective of the right to privacy: after a deep analysis of Article 8 of the European Convention of Human Rights and a brief digression through the main ECtHR judgments that expanded the meaning of the aforementioned ECHR's provision, the *Zakharov v. Russia* case, a landmark decision of the ECtHR that has raised profound questions regarding the scope and application of privacy rights within the European legal framework will be closely scrutinized.

In essence, chapter one lays the crucial groundwork for this comprehensive research into the dynamics of privacy in Europe. This chapter represents the cornerstone upon which the thesis will be built delving into the intricate theme of balancing security and privacy in the lives of European citizens.

From the theoretical and legislative point of view of the first chapter, as the second one will approach, the research will shift to a more historical analysis: indeed, chapter two will be a journey through some of the most important events happened in 2013 before and after the Snowden revelations.

As the former CIA contractor had revealed to the world the existence of several mass surveillance programs, the chapter will begin with a clear demarcation between bulk and targeted interceptions, illuminating the stark differences in their implications for privacy: theories behind the techniques, together with the European Court of Human Rights' opinions concerning the two different surveillance approaches, will be provided throughout the first paragraph.

Afterwards, the seismic event in the annals of privacy advocacy, that is to say the Snowden crisis, will assume center stage as its far-reaching consequences on governments, public opinion, and the international discourse surrounding privacy in the digital age will be analyzed. Within this context, the examination will linger on two critical surveillance programs: Prism and Tempora. These initiatives, unveiled through Snowden's disclosures, pierced the veil of secrecy that had shrouded governmental surveillance activities. Prism, a program operated by the United States' NSA, and Tempora, an endeavor undertaken by the GCHQ of the United Kingdom, came to symbolize the far-reaching extent of modern surveillance capabilities.

Furthermore, the critical role played by the USA PATRIOT Act of 2001[4] in birthing these surveillance programs will be illuminated. This pivotal legislation, enacted in the aftermath of the 9/11 terrorist attacks, introduced a legal framework that significantly expanded the powers of intelligence agencies, setting the stage for the surveillance practices that would later come to light through Snowden's revelations.

Finally, in order to provide a comprehensive view, the statements and positions of key United States politicians will be dissected, trying to unravel their perspectives on the surveillance revelations and their implications for national security, civil liberties, and global relations.

In sum, chapter two serves as a critical juncture in the research, revealing not only the historical underpinnings of surveillance practices but also the transformative impact of the Snowden crisis. Through an analysis of programs like Prism and Tempora, as well as the legislative framework that birthed them, we illuminate the profound consequences of these disclosures on governments, international relations, and the public's perception of privacy rights in the digital age.

The third and final chapter of this thesis will be dedicated to the pivotal case of *Big Brother Watch and Others v. United Kingdom*, an iconic legal battle borne from the revelations of Edward Snowden. Within this chapter, the applications and final judgment of the case, delving deep into the concurring opinions, particularly that of Judge de Albuquerque will be carefully dissected. As this intricate legal landscape will be traversed, the exploration will not conclude with the analysis of dissenting and concurring opinions alone. The attention will be also turned to a vital aspect that the Grand Chamber of the ECtHR left uncharted: the question of extraterritoriality. The analysis will shift on a thought-provoking inquiry into whether the right to privacy, as enshrined within Article 8 of the ECHR, can be extended beyond the borders of the Council of Europe. To shed light on this intricate matter, a series of precedents that have graced the docket of the ECtHR over the past two decades will be summoned forth. These cases, each with its own unique set of circumstances and contexts, will serve as signposts in the research, guiding it in the quest to unravel the boundaries and

[4] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, U.S. Federal Law, 26 October 2001.

potential applications of the right to privacy as safeguarded by Article 8 of the European Convention of Human Rights.

The chapter will reach its climax with a brief analysis of the parallel decision by the European Court of Human Rights in *Centrum för Rättvisa v. Sweden* trying to discern similarities and differences with the aforementioned *Big Brother Watch and Others v. United Kingdom* case.

This final chapter is indeed twofold: one path leads through the intricacies of *Big Brother Watch and Others v. United Kingdom* and *Centrum för Rättvisa v. Sweden*, trying to offer insights into the case's complexities and the diverse perspectives it has engendered; the other path guides to the unexplored terrain of extraterritoriality, where the footprints of privacy rights extend across borders and continents.

CHAPTER ONE

INTERCEPTIONS BETWEEN PRIVACY AND SECURITY: THE ECTHR'S PERSPECTIVE

1.1 Introduction

In our increasingly interconnected and digitalized world, the balance between personal privacy and collective security is a highly debated and controversial topic. As technology advances and redefines the boundaries of personal information, the conflict between the right to privacy and the need for security has intensified. While individuals demand for the preservation of their privacy as a fundamental right, governments and international organizations argue for increased security measures to address emerging threats which could undermine the society. For which it concerns the legal framework which has developed around these two competing interests, it poses an even more complex challenge, requiring careful consideration, ethical reflection, and a comprehensive understanding of the potential consequences of the decision taken by the different national legislators.

In this framework, the tragic events of 9/11 are crucial to comprehend the evolution of the concept of surveillance as we know it today. Indeed, terrorism did not come to the eye of the public in 2001 for the first time, but it surely paved the way to intelligent services to become the main tool to avoid new tragedies like the one of 9/11. The attacks, which killed more than 3000 people, started a global response: all the decisions made in the 9/11 aftermath concerned states' surveillance powers meant to avoid new threats from growing both abroad and within their own borders. Expanding surveillance

powers has its serious implications concerning human rights protection. Maintaining the status quo and silently fighting possible threats to peace by strengthening the surveillance on the society could challenge citizens' fundamental rights. Right to privacy in particular can be identified within the rights touched the most from those increased surveillance powers, which can be translated with an increased usage of mass surveillance and bulk interception methods.

The two aforementioned tools are different from other kind of instruments in the hands of governments to fight terrorism: detention, interrogations, and even torture mostly target individuals, while mass surveillance influences the whole society at once. Too much powerful surveillance powers could lead citizens to lose trust in the democracy itself: "the erosion of core aspects of individual privacy can fundamentally alter the nature of human behavior and interaction, our sense of personal freedom and the ethos of democratic societies"[5]. It is undeniable that nowadays countries need stronger surveillance tools to face growing threats, but the new surveillance practices, which started developing during the 9/11 fallout, together with the evolution of technologies, are challenging the notion of "right to privacy" itself, circumventing, or directly violating its constitutionality.

The dichotomy between surveillance and citizens' right to privacy surely is a topic of great importance. The increasing use of technology for surveillance purposes, combined with concerns about protection of personal data, has heated the debate about where the balance should lie between those two competing interests. On the one hand, security is without any doubt a precondition to a well working democracy: in an age where terrorist attacks and other forms of violence are becoming more common, it is essential for governments to have the ability to monitor and track individuals who pose threats to citizens. On the other hand, stronger surveillance measures represent a serious threat to individual privacy: excessive surveillance, little or no accountability, and low transparency undermine this fundamental right. Finding a solution to the dispute is not the purpose of this paragraph, but it would be useful to state the main issues of the debate in order to better comprehend the cases which will be closely analyzed throughout the development of this thesis.

[5] Lachmayer, K., & Witzleb, N., *The challenge to privacy from ever increasing state surveillance: comparative perspective* in *University of New South Wales Law Journal*, 2014, 37(2), 748-783.

The proportionality principle is the first, central, key issue while trying to find a balance between a protected private life and governments' interests for national security. Some authors define it as a set of rules which regulate the necessary conditions under which a protected fundamental human right can be limited: if certain conditions of national security are not reached, and there is not a clear danger to public safety, the right cannot be limited. On the opposite, other authors consider it as a principle which limits the actions of governments while searching for possible threats. The duality of proportionality presented here above helps to explain the real meaning of the principle: proportionality permits to protect the right to privacy, but at the same time to justify its limitation in certain situations[6]. Some criticisms to the principle argue that even in cases where highly intrusive surveillance measures are deemed as necessary, there is still a risk that they will be used inappropriately or excessively, leading to the loss of meaning of the right to privacy itself. This complex issue would need well developed guidelines which could help the public opinion to know when and how strong surveillance measures can be used and permitted.

This brings to the second key issue in the debate within right to privacy and security necessities: the question of consent. It is in fact known that the majority of the surveillance practices are carried out without the knowledge or consent of those being monitored. Even if mechanisms of notification have been established to permit individuals to know about an investigation being conducted to their regards, when it comes to bulk interceptions, as it will be closely examined in the next chapters, the situation becomes more complex: it is in fact impossible to notify thousands of citizens at the same time. Moreover, when it comes to public safety, sometimes consent would not be deemed as necessary for secret services to operate.

The third critical issue is accountability. Operating secretly is a precondition of the existence of the secret services: protection of sensible information and operational details are essential for intelligence agencies to conduct their work. But little oversight or public scrutiny could bring to possible abuses of power, violations of fundamental rights, or more generally, operations carried outside the bound of the law. Lack of transparency can also lead to the loss of mutual trust between citizens and the

[6] Milaj J., *Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance* in *International Review of Law, Computers and Technology*, 2016, 30(3), 115-130.

institutions which carry out surveillance. Anticipating one fundamental aspect of the Zakharov v. Russia case, in order to balance between the need of secrecy of intelligent services and the request of transparency from citizens, it is in principle desirable to entrust an independent and non-political body with the power to monitor intelligence agencies in order to ensure that the latter operate within the bounds of the law not being rigged by political influences[7].

Considering "security" as a precondition for a well working democracy, governments around the world have developed quite strong legal systems which sometimes may translate in violations perpetrated by states against citizens' fundamental right to privacy. In order to understand the complex framework of the right in Europe, it will be fundamental to firstly clarify how the right to privacy is regulated both at a national and at a European level: indeed, in the next paragraph it will be analyzed how this right is treated in several national constitutions and legislations.

Then, from a detailed inspection of the Charter of Fundamental Rights of the European Union, information on how the right is protected within the European legal framework will be provided. In the same paragraph, the 2014 European Court of Justice judgement of *Digital Rights Ireland Ltd v. Minister for Communication et al and Kärtner Landesregierung,* considered to be the very first turning point in the history of the protection of the right to privacy, will be briefly examined.

Following, the European Court of Human Rights point of view for which it concerns the right to privacy will be brought to the attention of the reader: art. 8 of the European Convention of Human Rights, together with the main European Union Directives and regulations concerning citizens' privacy disclosed during the last 30 years will be closely analyzed. In this paragraph, the 2015 *Roman Zakharov v. Russia* case will be brought in the foreground. As it will be deeply reviewed, the landmark decision of the European Court of Human Rights which followed the abovementioned case set a European standard to be followed in the future judgments concerning the right to privacy.

[7] van der Sloot B., *The quality of law: How the european court of human rights gradually became a european constitutional court for privacy cases*, in *J. Intell. Prop. Info. Tech. & Elec. Com. L. 160*, 2020, 11(2).

Finally, in the last paragraph of this first chapter, some conclusions will be drafted in order to briefly summarize the information provided in the previous paragraphs.

1.2 European Coordinates

Right to privacy has a particularly complex legal framework. If on the one hand each European country has its own laws and regulations governing privacy, on the other hand, there exist several guidelines established from regional organizations in order to permit a wide and uniform protection of the right across the European borders. Trying to explain how each country in Europe deals with the right to privacy would need more than one single paragraph, but in order to understand what is the direction towards which the majority of the European countries are redirecting their legal frameworks, it would still be useful to underline some of the main European national regulations concerning the abovementioned right. This brief phase will include four right to privacy legal frameworks from different European countries: Italy, France and Germany will be the first three countries covered in the following part in order to give the reader an overall knowledge on how the right to privacy is protected in Europe. Ultimately, the United Kingdom will be taken into the analysis too since the country is at the center of the *Big Brother Watch and Others v. the United Kingdom* case, the judgement which shaped the most recent European right to privacy framework.

1.2.1 *Right to privacy in Italy*

To begin, the Italian regulations of the right to privacy permit to understand how deep the protection of the right is, and how European countries are gradually conforming their legislations to more uniform European standards. Overall, it can be stated that Italy has a strong legal framework concerning the right to privacy which includes constitutional provisions, national laws, and regulations. Moreover, it must be underlined that Italy, because of its dualistic approach to international law, implements provisions contained in international treaties in national law before directly applying them on its citizens. In particular, Italy is bound by all EU legislation: the majority of the national laws and provision ever enacted within the Italian legal framework were

meant to standardize Italy to the European standard set in the various European Directives and Regulations ordered by the European Union through the years.

Concerning the constitutionally protected side of the right to privacy, within the first set of rights and duties of the citizens, from Art. 13 to 28, some references to citizens' privacy can be witnessed. Art. 14 in particular underlines the existence of an inviolability of people's home and personal domicile, while the purpose of Art. 15 of the Italian Constitution is to grant the safeguard and secrecy of each form of communication starting from the more traditional one: written correspondence. Particularly, Article 15 states that "*Freedom and secrecy of correspondence and other forms of communication are inviolable. Restrictions thereto may be imposed only by judicial decision stating the reasons and in accordance with guarantees established by law*"[8]. The provisions of the Italian first source of law states that everyone has the right to the inviolability of their person and correspondence. This means that individuals have a fundamental right to be free from interference or intrusion in their personal communications as well as their homes. As it can be drafted from the articles, rights of inviolability of one's home and freedom and secrecy of communication prescinds from being an Italian or foreign citizen, a minor, or a stateless person because of the lack of a precise reference on who could enjoy the right: the rights exist as such, and they can be expanded to collective subjects as well[9]. Limitations to the rights can be made but only by judicial bodies which must state the reasons behind the limitation and in accordance with the guarantees established by the Italian law.

In addition to the Constitution, Italy has several laws protecting privacy: as anticipated in the previous lines, most of them were established in order to comply with European Regulations and Directives. Law 675 of December 1996, or more commonly "privacy law", on the "Protection of people and other subjects concerning the treatment of personal data" was promulgated in order to comply with Directive 96/46/EC of the European Parliament: in particular, the law established an independent administrative authority, the "Italian Data Protection Authority" (IDPA), or "Garante della Privacy". Law 675 was subsequently repealed between 2003 and 2004 through the Consolidation Act in order to implement the "Personal Data Protection Code" (PDPC or DPCode)

[8] Art. 15, Italian Constitution.
[9] Califano, L., *L'articolo 15 della Costituzione*, 2022. [Online]. Available at: https://lamagistratura.it/commentario/lart-15-della-costituzione/.

which initiated a more correct regulation of the IDPA. The DPCode sought to unify the data protection framework, conversely to its predecessor, which primarily regulated specific data processing. It introduced conduct guidelines for journalistic, historical, scientific, or statistical activities. Initially, from the adoption of the first privacy Law no. 675/96 until 2011, the data protection provisions applied to both natural and legal persons. However, with the introduction of a new multipurpose act (Law no. 214/2011), the definitions of "personal data" and "data subject" were modified, narrowing the scope of the law exclusively to natural persons. Additionally, the DPCode includes rules and measures specifically addressing controllers involved in processing operations carried out with electronic tools for system administrators' tasks. Therefore, the implementation of the directive incorporated supplementary provisions to govern these aspects.

Several national laws were then passed by the Italian governments through the years in order to build a stronger legal landscape concerning citizens privacy: firstly, the 2012 legislative decree no. 69 which introduced the "personal data breach" concept, setting obligations to be fulfilled by providers of publicly available electronic communications in case of such data breaches. Within the essential obligations set out in the 2012 legislative decree the duty to notify the happening of a data breach to the Garante and the affected users can be witnessed.

The evolution of the Italian privacy legal framework continued with the adoption in 2015 of a Declaration of Internet Rights which contained several guidelines for future legislative efforts, and law 167 of 2017. The just mentioned law 167, or "Legge Europea 2017", was highly criticized for ruling against the case law of the European Court of Justice. Indeed, the Italian provision set the possibility for telecommunication operators to retain telephone and internet data up to 6 years[10].

Finally, in august 2018, law 167 was repealed and the previously mentioned DPCode was emended, charging the Italian Data Protection Authority as the supervisory authority responsible for monitoring and applying the 2016 European Union regulation concerning personal data and privacy known as "General Data Protection Regulation".

[10] Custers B., M. Sears A., Dechesne F., Georgieva I., Tani T. & van der Hof S., *EU Personal Data Protection in Policy and Practice*, in *Information Technology and Law Series*, Springer, 175-191, 2019, (29).

1.2.2 *Right to privacy in France*

Conversely to the Italian case, France has a monistic approach towards international law: this means that there is no requirement for international treaties to be incorporated into national legislation in order for them to become enforceable, even if, as it will closely be examined throughout the paragraph, an effort to homogenize the French legal landscape to a European standard can still be witnessed.

Protection of the right to privacy in France is indeed another example of a perfect mixture between national provisions and European regulation even if the legal framework of the right in the francophone country is quite different from the Italian case. The main difference with the Italian provisions is that there is no specific personal data protection or privacy guarantee in the 1958 Constitution. Actually, in the French Constitution there is no article referring to human rights at all: provisions concerning human rights are contained in the preamble of the Constitution. When dealing with the right to privacy in France, the main provision which must be taken into the account is the July 1970 Act of Parliament which modified both the Criminal and Civil Codes: the law defined a new framework concerning possible violations or offences to the privacy of the citizens and the consequent sanctions[11]. Historically, about one century before the aforementioned act, right to privacy in France was slightly different: the term "private life" within the French boundaries appeared in 1819 for the first time, and even before that, art. 675 of the Civil Code referred to the right to privacy only when dealing with the neighbor of the person concerned as it stated that "One of the neighbors may not, without the consent of the other, install any window or make any opening in the dividing wall, in whatever manner possible, even by using opaque glass"[12].

For which it concerns the French Civil Code today, the new article 9 states as following: "*Everyone should be able to expect their privacy to be respected. The judge may […] prescribe any measure […] with a view to preventing or bringing to an end an intrusion into the intimate nature of the private life of an individual. These measures may be implemented by the judge as emergency measures if necessary*"[13]. As it stands, article 9 is focused on the reasons why a judge would decide to end possible

[11] Trouille H., *Private life and public image: Privacy legislation in France* in *ICLQR*, 2008, 49(1), 199-208.
[12] Wagner, W. J., *The Development of the Theory of the Right to Privacy in France* in *Washington University Law Quarterly*, 1971, 1971(1), 45-72.
[13] Art. 9, French Civil Code.

interferences with the privacy of individuals. On the other hand, the framework described in the French Criminal Code is quite more complex: the 1970 Act updated five articles from 368 to 372 with the aim of not only describing what are the possible intrusions that an individual could pursue in order to infringe someone's privacy, but the possible sanctions too.

It is worth to be mentioned that some exceptions to the abovementioned laws exist: state of emergency in the country permits momentaneous violations of people's privacy in the search of possible threats to the life of the citizens. State of emergency in France has a complex history: this special legal regime was established with a legislative act in 1955. This state of exceptional powers, which concerns privacy issues too, was imagined in order to deal with insurrections in Algeria, a French colony at the time. The state of emergency regulation, again proclaimed in 2015 after the sadly well-known terrorist attacks of the Stade de France and the Bataclan, permits house searches and seizure of electronic data without need of a formal search warrant[14].

Personal data protection in France is regulated mostly through sectoral provisions: online electronic communication services are regulated through Article 34 and following of the Postal and Electronic Communications Code, consumers rights to privacy are policed by Articles 223 and 224 of the Consumer Code, the Public Health Code administers the processing of health data, while the retention of data contained in public archives is ruled by the Property Code.

To conclude with the French case, as a member of the European Union, the francophone country has its own interpretation of the previously mentioned European General Data Protection Regulation, that is to say the so-called French Data Protection Act. Although initially promulgated in 1978, the Act was deeply emended throughout the years in order to comply with the European Directives: the first modification of this provision was made in 2004 and the second one more recently, in 2018, in order to uniform the French legislation concerning privacy with the GDPR. As it stands, the French Data Protection Act poses some fundamental obligations to individuals and organizations under that specific law: processing personal data must have relevant legal and financial reasons, data handlers must provide clear and comprehensible information

[14] Vauchez, S., *The State of Emergency in France: Days Without End?* in *European Constitutional Law Review*, 2018, 14(4), 700-720.

about their privacy policies and must gain explicit consent in order to process private data. Moreover, together with the guidelines on how to deal with data breaches, the FDPA specifies the conditions under which private information could be transferred abroad. Few are the government direct intervention in the right to privacy legal landscape during the last decade: worth to be mentioned are the 2014's publication of a public data policy aimed to make the French administration more transparent and accountable, and the September 2015's "Project de Loi pour une République Numérique", a co-worked with the citizens law-drafting project which contained more detailed provisions about net neutrality, data portability, confidentiality of private communications online, the right to be forgotten, and the openness of public data. The latter was translated in law in 2016.

As the Italian case, France has an independent body commissioned with the duty to apply the rule complying with the European requests: the so-called Commission Nationale de l'Informatique et des Libertés or *CNIL*. The French data protection authority created the so-called "Le collective Educnum" in 2013, a platform which united several organizations with the aim to raise the public awareness on personal data protection[15]. As it can be witnessed, the CNIL was not formed in order to comply with European Directives: it was already well working in 2018 when the European GDPR was enacted, but it was strengthened by the same year's bill with new competences in order to apply the European Parliament will. Within its new powers the CNIL now has stronger investigation means, and the ability to elaborate "soft laws" such as guidelines, recommendations, and standards to be followed by French individuals or collectives[16].

1.2.3 *Right to privacy in Germany*

Although, in some respects, similar to the previously analyzed cases, Germany represents a peculiar case within the European Union borders. The complexity of the German case can be immediately witnessed by analyzing the structure of the German federal Constitution, or better, the German Basic Law: if on the one hand the principal

[15] Custers B., M. Sears A., Dechesne F., Georgieva I., Tani T. & van der Hof S., *EU Personal Data Protection in Policy and Practice*, cit., 137-151.
[16] Tambou, O., *France: The French approach to the gdpr implementation. European Data Protection Law Review* in EDPL, 2018, 4(1), 88-94.

German source of Law outlines specific areas of responsibility exclusively held by the federation, on the other hand, all other responsibilities, including legislative authority, remain under the jurisdiction of the individual states. In terms of privacy and data protection, both the federal government and the state governments have the authority to pass laws and oversee compliance. To better comprehend the peculiarity of the German Federation, when the European Union placed the first fundamental dowel for the right to privacy protection in Europe, the enacting of the EU Data Protection Directive 95/46/EC, 16 states of the German federation anticipated the federal German legislators in implementing the Directive[17].

For which it concerns the concrete protection of the right to privacy, it is somehow federally protected but not directly: Article 10 of the Basic Law refers to the privacy of correspondence, posts, and telecommunications and the circumstances under which those inviolabilities may be restricted[18], but there is no explicit reference to the mere existence of a "right to privacy". In the nebulous right to privacy legal framework of the German Basic Law, it becomes fundamental to underline the importance of article 2. The article in question underlines an inviolability of the personality of the people: "*Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law. Every person shall have the right to life and physical integrity. Freedom of the person shall be inviolable. These rights may be interfered with only pursuant to a law*"[19]. According to Professor Harold Cooke Gutteridge, the right to freely develop a personality can be analyzed in multiple ways. In particular, the author underlines that "the law must be such as to protect the individual to the fullest extent in the exercise of his faculties in every conceivable direction. The individual is therefore entitled to complain of any unauthorized interference […]. In short, any willful and unauthorized incursion by others into the private life of an individual is *prima facie* to be regarded as an actionable wrong"[20]. As it can be drafted from Professor Gutteridge words, right to privacy is indeed an integral part of right to freely develop a personality: using the words of the American jurist Samuel Warren and the former judge of the American

[17] Custers B., M. Sears A., Dechesne F., Georgieva I., Tani T. & van der Hof S., *EU Personal Data Protection in Policy and Practice*, cit., 49-71.
[18] Art. 10, German Basic Law.
[19] Art. 2, German Basic Law.
[20] Gutteridge H., *The comparative law of the right to privacy* in *Law Quarterly Review*, 1931, 47(2), 203-218.

Supreme Court Louis Brandeis "privacy is one of many dowels being part of an individual's personality"[21]. In conclusion, since right of personality is protected in the German Basic Law, right to privacy follows the same faith[22].

As the previously analyzed countries, Germany, as a member state of the European Union, has enacted federal act aimed to comply with the European Parliament decisions. The 1995 European Directive was the first deep modification to the European right to privacy legal landscape. As anticipated, it took some years for the German legislators to federally implement the provisions and obligations contained in the 1995 Directive: after being anticipated by 16 states of the Federation which regionally implemented the European law, in 2001 an official federal legislation came into force. Two amendments were passed in 2003 and 2009 which mainly aimed to regulate the duties of privacy officers (2003) and to facilitate judges in cases concerning private data (2009). The more recent *Bundesdatenschultzgesetz* or New Federal Data Protection Act of 2018 was indeed designed in order to apply to the German country the decisions of the GDPR. The FDPA established the creation of a Federal Commissioner for Data Protection and Freedom of Information which main aim is to check on the data protection in public offices, corporations, and in telecommunication and postal services. At the same time, the new established body has the duty to inform citizens about data protection level in the country[23].

1.2.4 *Right to privacy in the United Kingdom*

As last example of European country protecting the right to privacy, the United Kingdom case has been accurately selected in order to give the reader a wider consciousness of various different legal frameworks concerning this right. UK presents a dissimilar legal framework from the other analyzed here above: as it is well known, the United Kingdom not only does not have a written Constitution since its legal system is based on the Common Law model, but there also exist three distinct legal systems

[21] Warren S. and Brandeis L., *The right to privacy* in *Harvard Law Review*, 1890, 4(5), 193-220.
[22] Lehman J. A., *The right to privacy in Germany* in *New York University Journal of International Law and Politics*, 1968, 1(1), 106-127.
[23] Custers B., M. Sears A., Dechesne F., Georgieva I., Tani T. & van der Hof S., *EU Personal Data Protection in Policy and Practice*, cit., 49-71.

for England and Whales, for Northern Ireland, and for Scotland. Despite that, several laws apply across the country.

In the following part of the paragraph, right to privacy will be analyzed from several European Organizations or Conventions perspectives, but in order to deal with the UK case, an anticipation is needed: the 1950 Human Rights Convention in Rome, of which art. 8 recognizes a right to privacy, easily translated to local Constitutions in the years following its entry into force. On the contrary, despite the dualistic approach of the UK in dealing with international law, Great Britain legal system had its troubles in incorporating the Convention in its everyday life: courts in the UK did not have the possibility to directly apply the Convention because of the absence of a domestic written constitutional text. The complex legal framework which arose in the United Kingdom in the fifty years following the signature of the European Human Rights Convention paved the way for the 1998 Human Rights Act, which came into force in 2000. The act in question permitted to easily incorporate in the British domestic legal system all the internationally recognized principles listed in the Human Rights Convention, including right to privacy[24]: more precisely, once the Act came into force, violations of fundamental human rights listed in the text of the European Convention of Human Rights could be brought before UK courts.

To this regard, English courts faced several cases concerning the new signed Human Rights Act in the years following: from *Douglas v. Hello!, Ltd* to *Campbell v. Mirror Group Newspapers Ltd*, concluding with the landmark case of *Mosley v. UK* The above-mentioned cases permitted the development of a stronger legal base concerning the right to privacy even in a country where the legal system is based on a Common Law model[25].

1.3 Right to Privacy Within the European Union Legal Framework

At the European Union level, the theme of the right to privacy has been largely dealt by European lawmakers. Since the 1990s, the European Union has been supplied with

[24] Mance J., *Human Rights, Privacy and the Public Interest—Who Draws the Line and Where?* in *Liverpool Law Review*, 2009, 30, 263-283.
[25] Stanley J. E., *Max Mosley and the English right to privacy* in *Washington University Global Studies Law Review*, 2011, 10(3), 641-668.

a deep legislative framework concerning the privacy with a great number of Directives and Regulations: Directive 96/46, and more recently, its legal successor, the 2016 General Data Protection Regulation (GDPR), permitted European lawmakers to regulate the complex legal framework concerning the right to privacy. Moreover, privacy rights have been constitutionalized in the EU primary source of law with articles 7 and 8 of the European Union Charter of Fundamental Rights in 2000.

For which it concerns Directive 96/46, or "Data Protection Directive" (DPD), it aimed to grant a free flow of data across the boundaries of the members of the Union, assuring that the processing of this data could be operated only respecting certain specific "qualitative principles": within those principles, the most worthy to be mentioned are the already well treated proportionality principle, which forces the processing of data to be proportional to the purpose that prompted the initiation of the investigation, and the absolute acknowledgment and consent of the ones being object of an investigation. Moreover, the DPD imposed on the states members of the Union to establish independent authorities empowered to oversee the processing of data in order to comply the national legislations with the EU principles enshrined in the Directive[26]. The just mentioned obligation has been indirectly analyzed in the previous paragraph: as it has been stated before, Italy enacted Law 675 in 1996 establishing the Italian Data Protection Authority and France already had the French Data Protection Act since 1978, which was modified *ad hoc* to comply with the European Directives throughout the years. In turn, the General Data Protection Regulation of 2016 is substantially an update of the former Directive 96/46 by regulating the process under which individuals, companies, or organizations deal with private data of individuals within the European Union's borders[27]. Previously, it has been analyzed how Germany tried to comply with the GDPR principles with the New Federal Data Protection Act of May 2018.

The European Charter of Fundamental Rights, which came into force in 2009, is a legally binding document that sets out the fundamental rights and freedoms of

[26] Fabbrini F., *The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court* in de Vries S. (ed), *Five Years Legally Binding Charter of Fundamental Rights*, iCourts Working Paper Series, No. 19, 2015, [Online]. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2576214.

[27] European Commission, *What does the General Data Protection Regulation (GDPR) govern?*, 2016 [Online]. Available at: https://commission.europa.eu/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en#:~:text=References-,Answer,to%20individuals%20in%20the%20EU.

individuals within the European Union. It was proclaimed and signed in December 2000 by the EU institutions and member states. The text surely is the most important, legal binding source of law of the European Union, it is based on the values and principles shared by EU member states and reflects the Union's commitment to the protection and promotion of human rights. It guarantees a broad range of civil, political, economic, and social rights that apply to all individuals within the jurisdiction of the EU. The Charter finds its inspiration from a diverse range of influences, including global human rights instruments like the Universal Declaration of Human Rights and the European Convention on Human Rights, of which a closer examination will be made in the next paragraph, as well as the national constitutions of EU member states. Additionally, it considers the precedents set by the European Court of Justice and the European Court of Human Rights in its interpretation and application.

The presence of articles which make a direct reference to the right to privacy can be witnessed within the very first pages of the legal text. In particular Article 7 and Article 8 of the European Charter of Fundamental Rights are the main provisions that protect individual rights and freedoms within the European Union. Art. 7 focuses on the private life of individuals: "*Everyone has the right to respect for his or her private and family life, home and communications*"[28]. While art. 8 underlines the importance of the protection of personal data: "*Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified*"[29].

These two articles in particular are at the center of the reasonings of one of the pillar cases concerning right to privacy of the last decade: *Digital Rights Ireland Ltd v. Minister for Communication*. The European Court of Justice (ECJ) has always adopted a strict method of scrutiny when dealing with member states' legislations concerning the right to privacy and possible violations of articles 7 and 8 of the European Union Charter of Fundamental Rights. The *Digital Rights Ireland* case marked a pivotal moment in the European Union's efforts to protect digital privacy right. Indeed, the court embraced a different method, checking directly on the Directives proposed by the

[28] Art. 7, Charter of Fundamental Rights EU.
[29] Art. 8, Charter of Fundamental Rights EU.

EU political branches of government: the ECJ took the unheard-of step of invalidating an entire piece of EU legislation for a violation of the aforementioned articles 7 and 8[30].

The case, which unfolded against the backdrop of growing concerns over surveillance and data retention, centered around the legality of the Data Retention Directive and its compatibility with articles 7 and 8 of the Charter. The 2006 Directive, direct consequence of the Madrid massacres of March 2004, laid down the obligation on the providers of publicly available electronic communications services or of public communications networks to retain the telecommunication data, which are generated or processed by them, necessary to identify source, destination, date, time and duration of a communication, the equipment with which the user sent the communication and his location. Before the Directive was promulgated, not only telecommunication providers could not retain private data, on the opposite they were obliged to erase this data as a general rule. In particular, the Directive stated that member states were obliged to control that sensible, private data was retained for not less than 6 months and for a maximum of 2 years, giving on the one hand security authorities a powerful tool to investigate and reprime crimes, but on the other hand clearly impacting on the right to privacy.

The Directive did not have an easy life from its early stages: Ireland voted against the legislation deeming it too intrusive, but the Irish country's complaint based on the competence of the EU political branches of applying such legislation was rejected. Nonetheless, some national Constitutional Courts decided to invalidate domestic legal measures taken to implement the European Directive: an advocacy group known as Digital Rights Ireland Ltd. challenged the Directive on the ground that it violated several fundamental rights, including the right to privacy and protection of personal data enshrined in the EU Charter of Fundamental Rights. Their challenge pushed the Irish national Constitutional Courts to pose questions of constitutionality to the ECJ about whether the Data Retention Directive was compatible with the rights to privacy of family lives and the protection of personal data as articles 7 and 8 of the Charter underlined.

[30] Fabbrini F., *The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court,* cit.

The key arguments brought by Digital Rights Ireland Ltd. Were the following: a clear violation of principles of necessity and proportionality, a possible interference with freedom of expression and association, and the lack of harmonization in implementing the Directive across member states. The answers to the constitutionality questions were found by the ECJ within the articles of the same Charter of Fundamental Rights, more precisely in article 52: the article in question explains how and to what extent these rights can be limited. In particular art. 52 states that "*Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others*"[31]. According to the work of the ECJ, in order to enter into force, the European Directive 2006/24 should have respected 3 main criterions which are engraved in article 52 of the Charter: do not overcoming the essence of the rights listed in articles 7 and 8, meeting an objective of general interest, and being strictly necessary to reach that objective by correctly balancing between the need of security and the privacy of the citizens.

For which it concerns the first two criterions, the court not only declared that the Directive did not affect the essence of the two fundamental articles of the Charter, but also stated that pursuing public security by fighting international terrorism constituted a fair objective of general interest to apply the Directive.

The Court's opinion run against the Directive when it dealt with its necessity in the fight to international terrorism: its negative point of view concerning the necessity of the Directive can be witnessed from paragraphs 51 to 68 of the final paper of the judgment. The ECJ considered that the retention of data, even if made under the cloak of searching for possible threats, went well beyond the crimes themselves. The access to the retained data too was not regulated enough, paving the way to a too broad access permission to non-specified bodies. According to the court, the timeframe for the retention of data was not sufficient: there was no clear distinction of time between different categories of data.

[31] Art. 52, Charter of Fundamental Rights EU.

Finally, the last point underlined from the court suggested the existence of an incorrect protection of the data retained: in the text of the Directive there was no provision which prohibited the competent authorities to give the data to countries with a lower capacity of protection of digital data, giving this way an easier access to private information by unlawful actors[32]. The so-called "necessity test" built by the Court was not passed by the Directive. In consequence, the points underlined here above were enough for the court to struck down the Directive, completely eliminating it from the EU legal order.

The ECJ decision in *Digital Rights Ireland Ltd v. Minister for Communication et al and Kärtner Landesregierung* permits to comprehend the European Union's most important legal body point of view concerning the right to privacy. Parallelly, the European Court of Human Rights too has built an enormous legal framework around the right to privacy: if on the one hand *Big Brother Watch and Others v. the United Kingdom* of 2021 can be considered as the peak of the ECtHR work, the basis of its reasoning was built six years before. In the next paragraph, art. 8 of the European Convention of Human Rights (ECHR) together with the 2015 *Roman Zakharov v. Russia* case will be closely analyzed, in order to give to the reader a deeper consciousness of the European right to privacy legal framework.

1.4 The ECtHR's Perspective: *Zakharov v. Russia* and the Setting of a European Standard

1.4.1 *Art. 8 of the European Convention of Human Rights*

Before analyzing art. 8 of the ECHR and its strictly connected *Roman Zakharov v. Russia* case of 2015 a brief clarification is needed: it must be clear why it has been decided to separate the European Court of Human Rights perspective from the previous paragraph concerning the right to privacy within the European Union. The answer is quite simple: the European Court of Human Rights (ECtHR) is indeed an independent judicial body established under the European Convention on Human Rights (ECHR). It operates independently from any political influence or control in order to ensure the

[32] Case of *Digital Rights Ireland Ltd v. Minister for Communication et al and Kärtner Landesregierung*, Judgment of the European Court of Justice of 2014.

impartial and effective enforcement of human rights. The court's independency is not only to be considered from national governments or institutions, but also from the Council of Europe itself.

The Convention which established the ECtHR, guarantees a wide range of civil and political rights to individuals within the jurisdiction of the member states. It sets out fundamental rights and freedoms, including the right to life, the prohibition of torture, the right to liberty and security, the right to a fair trial, the right to privacy, freedom of thought, conscience and religion, freedom of expression, and the right to marry and found a family, among others. For which it concerns the subject of major interest for this thesis statement, right to privacy, the provision concerning the right can be identified in art. 8 of the Convention. Art. 8 of the ECHR is without any doubt the most known guarantee against any kind of abuse of citizens private life. The text of the aforementioned article presents both the passive rights enjoyed by the citizens, of which the primary purpose is to defend them from any arbitrary interference in their private life conducted by public authorities, and the possible exceptions under which a limitation of the right can be permitted: "*Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of other*s"[33]. The wording "*to respect for*" does not alter the fundamental nature of Article 8, which, similar to other provisions within the Convention, primarily serves as a right aimed at countering interferences by the State. The main objective of this article is to safeguard individuals against arbitrary intrusions by public authorities into their private and family life. It goes beyond simply requiring the State to refrain from such interference. In addition to this core negative obligation, there are also positive obligations that arise from the need to effectively respect private and family life: like other provisions within the Convention, Article 8 entails the responsibility of the State to safeguard individuals from infringements on their fundamental rights by

[33] Art. 8, European Convention of Human Rights.

third parties. Additionally, the Article imposes on the State the duty to ensure the provision of specific services, such as procedural guarantees.

Since the article is at the center of the next paragraph's case, *Zakharov v. Russia*, a further, closer, examination of the wording is needed. In particular, the focus wants to be directed towards the second paragraph of the article. The paragraph in question directly refers to the justifications which may be attributed to legally permitted interferences with the right perpetrated by member states or third parties: a possible interference is indeed permitted if it is in accordance with the law and necessary in a democratic society in the interests listed in paragraph 2 of the article. For which it concerns the requirement that any interference with the right to private and family life must be "*in accordance with the law*", it ensures that there is a legal basis for any limitations on this fundamental right. It means that interferences must be authorized by domestic legislation and not arbitrary in nature. This principle serves as a safeguard against abuses of power and ensures that individuals are aware of the legal framework within which their rights may be restricted. The law should be accessible, clear, and provide individuals with adequate protection and procedural guarantees. "*In accordance with the law*" also implies that the law should be predictable and not subject to arbitrary changes. Individuals should have a reasonable expectation of how their private and family life may be regulated by the state. The requirement for legal clarity and accessibility allows individuals to understand the scope of their rights and the circumstances under which interferences may be justified.

On the other hand, the concept of "*necessary to a democratic society*" recognizes that in certain circumstances, there may be legitimate reasons for interfering with this right. However, such interferences must meet certain criteria to be considered justifiable. To be considered necessary to a democratic society, the interference must pursue a legitimate aim, such as protecting national security, public safety, or the rights and freedoms of others. The aim must be important and in line with the values of a democratic society. The interference must also be proportionate, meaning that it must be the least restrictive measure available to achieve the legitimate aim. The state should demonstrate that there is a reasonable relationship of proportionality between the means employed and the aim sought to be realized.

Furthermore, the notion of a "*democratic society*" implies that limitations on rights must respect the core values and principles of democracy, including the rule of law, pluralism, tolerance, and respect for human rights. The interference should not undermine the essence of the right to private and family life and should strike a fair balance between the interests of the individual and the broader interests of society[34]. The just mentioned second paragraph of Article 8 of the European Convention of Human Rights will be vital for the comprehension of the reasoning behind the final judgment of *Zakharov v. Russia*. As the reader will notice, the standards set in the aftermath of the decision were based exactly on the two principles expressed by Article 8, para. 2 of the Convention.

If on the one hand the outcomes of *Zahkarov v. Russia* can be considered one of the most recent developments for which it concerns the European right to privacy legal framework, the evolutionary path of the legal landscape of privacy in Europe passed through several landmark decisions which shaped the fundamental right up to the present day.

Given that none of the international data protection documents provide an exhaustive definition of personal data, it is the responsibility of the Court to emphasize its boundless nature and determine whether specific information qualifies as personal data on a case-by-case basis. This was exemplified in the *Malone v. the United Kingdom* case, which revolved around the surveillance of the applicant's communications by the police through the monitoring of his telephone usage. The court arrived at a significant conclusion that data derived from such monitoring, including dialed numbers, constitutes an integral part of telephone communications. Consequently, it emphasized that the release of this information to the police without the subscriber's consent violated Article 8. In this instance, the European Court of Human Rights not only interpreted the extent of "personal data" by categorizing dialed call information as information linked to the individual, but also exerted a substantial influence on the accessibility and foreseeability principles pertaining to privacy and existing data protection laws.

The Court expanded the meaning of the expression "personal data" in another landmark decision identifiable in *Benedik v. Slovenia* where the Court established that

[34] Grabenwarter, C., European Convention on Human Rights. 1st edn. Bloomsbury Publishing, 2014.

information associated with dynamic IP addresses falls within the definition of personal data too.

Concerning the processing and possible dissemination of sensible information, the Court developed a clear jurisprudence: in *Z. v. Finalnd* and *M.S. v. Sweden* it was established that protection of personal data, both during the entire duration of criminal proceeding as well as during the action of transferring medical records to third parties, is essential in order to respect the right to private life guaranteed by Article 8 of the Convention.

To this regard, the case *P. and S. v. Poland* brought the Court to discuss about unauthorized disclosure of sensitive personal data by hospital staff to the media. The applicant, a fourteen-year-old woman who became pregnant following a rape had chosen to undergo an abortion. Although the information made public did not include the applicant's name or other specific details, the Court acknowledged that the disclosed information was sufficiently detailed to identify and locate the applicant: the reasoning brought the Court declaring that, to fall under Article 8 of the Convention, even anonymized-published information must contain enough specific details to establish the person's identity.

Moreover, in the 2007 case of *M.M. v. the United Kingdom*, which dealt with the retention of criminal data by authorities, the European Court of Human Rights reached the conclusion that the extent and sensitivity of the recorded information, as well as the scope of the recording system, are crucial factors in determining the importance of implementing appropriate safeguards during subsequent data processing stages. Once again, the Court underlined that the authorities responsible for the storage and disclosure of criminal record data bear the responsibility of ensuring the protection of private life of the citizens of a given country. This responsibility is particularly significant due to the nature of the data held and the potentially severe consequences which may arise from its disclosure.

While states are granted with a considerable discretion during criminal investigations, including the collection of sensitive personal data for extended periods, the European Court of Human Rights critically evaluates data retention practices and emphasizes the necessity of deleting data once it becomes irrelevant. This principle was highlighted in the 2008 case of *S. and Marper v. the United Kingdom*, where the court

noted that the processing of DNA profiles allows authorities to potentially determine the ethnic origin of the donor, and these techniques are indeed utilized in police investigations. The prolonged retention of the applicants' fingerprints, cell samples, and DNA profiles by the authorities, even after the completion of criminal proceedings, and the utilization of this data to ascertain their ethnic origin were deemed to infringe upon and violate their rights.

Worth to be mentioned is the 1987 *Laender v. Sweden* too which permitted the Court to build a stronger framework around the right to privacy: even though a concrete violation of Article 8, at the center of the case, was not found, the European Court of Human Rights observed that when public authorities store and disseminate information about an individual without providing an opportunity for that individual to challenge or refute the information, it constitutes an infringement on the right to privacy[35].

The decennial construction of the legal framework around the right to privacy in Europe has recently witnessed a crucial turning point in the landmark case of *Roman Zakharov v. Russia*. Indeed, as it will be closely analyzed in the next paragraph, the standards set in the 2015 decision are likely to change the jurisprudence around the right orienting the ECtHR approach towards national security interests at the expense of the privacy of the citizens.

1.4.2 *The Zakharov v. Russia case of 2015*

The wording "setting of a European standard" chosen for the title of the paragraph is not just a catchy phrase. As it will be closely analyzed in the next pages, *Zakharov* has had a great influence on the reasoning behind the *Big Brother Watch and Others v. the United Kingdom* case. Not only it could be stated that the Big Brother Watch case is an updated version of what was decided by the ECtHR in 2015: Big Brother judgement could not even have been existed without the decisions taken in the aftermath of the *Zakharov* case.

The *Roman Zakharov v. Russia* case is a landmark decision not only concerning the right to privacy legal framework: the particularity of the case can be immediately

[35] Kovalenko Y., *The Right to Privacy and Protection of Personal Data: Emerging Trends and Implications for Development in Jurisprudence of European Court of Human Rights*, in *Masaryk University Journal of Law and Technology*, 2022, 16(1).

witnessed from the admissibility of the application, but in order to comprehend the criteria which brought the application to be admitted by the ECtHR, it would be useful to state the facts that brought Mr. Zakharov bringing a claim before the European Court of Human Rights.

The applicant, Roman Andreyevich Zakharov, was the editor in chief of a publishing company. At the same time, he worked as the chairperson of the St. Petersburg branch of the Glasnost Defense Foundation, a non-governmental organization which main aim was to monitor the state of media freedom in the Russian regions. His claims were directed towards the legality of Order 70 of the Russian Ministry of Communications: the order in question required telecommunication networks to install equipment enabling law enforcement agencies to carry out operational-search activities and permitting the Federal Security Service to intercept all telephone communication without prior judicial authorization. Mr. Zakharov held that the new surveillance system established with Order 70 constituted a direct violation of the private life of the citizens, but Russian courts rejected his claims on the basis that he had failed to prove that his telephone communications had been intercepted. Once having exhausted the national remedies, Mr. Zakharov turned to the ECtHR where a similar admissibility question arose. In fact, according to the European Convention of Human Rights, the Court may only consider cases in which certain criteria are met: the applicant must have exhausted all the available domestic remedies and must submit the application to the court within six months from the final decision of the domestic authorities[36] (both the criteria are enlisted in art. 35 of the ECHR). Moreover, as it is stated in art. 34 of the ECHR "*The Court may receive applications from any person, nongovernmental organization or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto. […]*"[37] making clear that a concrete violation of the rights of the applicants must occur in order to submit any application to the European Convention of Human Rights. As the law stands, it seems that no review of the legislation could be made *in abstracto*, but the Court showed how previously some exceptions were made.

Behind this first reasoning it can be witnessed the consciousness of the Court that when dealing with secret surveillance cases it is not likely that an individual knows

[36] Art. 35, European Convention of Human Rights.
[37] Art. 34, European Convention of Human Rights.

about the interception with his private life conducted by national authorities. It followed that, once having recognized the nature of secret surveillance, the Strasbourg Court used its earlier jurisprudence to choose the approach to be maintained towards Roman Zakharov's application. The Court's approach relied specifically on two previously sentenced cases: *Klass and Others v. Germany* and *Kennedy v. the United Kingdom*. Trying to harmonize the approaches, the Court held that secret surveillance systems must not end up being effectively unchallengeable meaning that it could not be left a free highway for the intelligent services to operate without being supervised by a judicial body. Moreover, the principle accepted by the ECtHR was that the challenge could be directed towards legislation itself, rather than a specific instance of interception. This challenge could be made if the applicant belonged to a group potentially affected by the rules in question, while also considering the availability of remedies. In cases where effective remedies were absent, the legislation could be challenged without the need for the applicant to demonstrate a specific risk of surveillance based on their personal situation. In the case of Mr. Zakharov and the Russian system, since there were no effective remedies, it was not necessary for him to prove that he was personally at risk of surveillance[38]. It followed the admission of the application from the ECtHR based on the recognition of the influence of the legislation to every user of communication regardless any proof of them being directly intercepted: in some cases, just the fact that a law exists, may give the possibility to the applicant to submit some claims for possible violation of his rights to the ECtHR.

Once having established under which conditions the Court decided on the admissibility of the case, its merit can be finally taken into the account: the Court was indeed called to control for a possible violation of art. 8 of the European Convention of Human Rights. To recall what art. 8 of the European Convention of Human Rights underlines, generally there cannot be any interference with the right, but some exceptions may occur: any law limiting the scope of the right or any operation conducted by public authorities which could interfere with the privacy of the citizens must be done in accordance with the law, in the interests of national security, public safety, or economic well-being of a country, and it must be necessary to a democratic

[38] Woods L., *Zakharov v. Russia (Eur. Ct. H.R.)* in *International Legal Materials*, 2016, 55(2), 207-266.

society. In the long text of the decision of the Court, paragraphs from 227 to 302 contain the reasoning regarding the three main aspects listed here above.

To begin, the court analyzed the wording "*in accordance with the law*" and its intrinsic meaning. To briefly summarize what has been underlined in the previous paragraph, domestic law must meet quality requirements: it must be accessible to the individuals and foreseeable as to its effects: a law should be clear and detailed in order to be well understood by citizens. Moreover, it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. This means that any law should contain criteria to limit and drive the discretion of public authorities to prevent any form of abuse of power.

To this regard, the European Court of Human Rights' work brought the establishment of the so-called "Weber criteria", six standards which any law limiting the scope of the right to privacy must respect in order to be passed by the legislators of each of the contracting states of the Convention. The Court referred to those criteria as "minimum safeguards that should be set out in law in order to avoid abuses of power"[39].

First of all, the Court assessed the nature of the offences which may give rise to an interception of private data order: in para. 244 the Court recognized that any state should not be obliged to exhaustively list all the specific offences which may pave the way for an interception order. However, still "sufficient detail should be provided on the nature of the offences in question"[40]. According to the 1995 Russian Operational-Search Activities Act (OSAA) and the 2002 Code of Criminal Procedure (CCrP), the Court underlined, communications made by Russian citizens could be object of interceptions in cases of offences of medium severity, serious offences, and serious criminal offences. While on the one hand the Court considered sufficiently clear the way Russian legislation specified the kind of offences which could give authorities a reason to start any form of interception, on the other hand it was concerned by the fact that the same legislation permitted secret services to conduct intercepting operations even for less serious crimes: pickpocketing, as example. Furthermore, for which it concerns events or activities which could potentially undermine Russia's national, military, economic or ecological security, "the OSAA does not give any indication of

[39] Case of *Roman Zakharov v. Russia*, Judgment of the European Court of Human Rights, 2015, para. 231.
[40] Case of *Roman Zakharov v. Russia*, cit., para. 244.

the circumstances under which an individual's communications may be intercepted […] leaving the authorities an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse"[41].

Following, the Court stressed that any law interfering with people's privacy should have clear references to who are the categories of citizens that can intercepted by the competent authorities and for how long: any interception must be limited in time, otherwise it may lead to a serious abuse of power. Concerning this aspect, the Court was partially satisfied by the Russian legislation: both in OSAA and CCrP a clear time span of a maximum duration of six months of an interception is set out. Russian codification also contains a clear reference about a possible renewal of the authorization of interception. On the contrary, the Court noticed that the circumstances in which the interception must be discontinued when no longer necessary were only specified in the CCrP and not in the OSAA. This could possibly lead to an arbitrary interference of the public authorities.

The fourth criteria set by the Court concerned the procedure to be followed by the Russian authorities to collect, store, and analyze the data: the Court found the Russian legal framework sufficient since it provided enough guarantees for the data to not be accessed by unauthorized individuals[42]. Moreover, the storage of a maximum time limit of six month before the complete elimination of the data collected was considered reasonable by the justices of the ECtHR.

Finally, the last two criteria focused on the precautions to be taken by secret services when sending private information to third parties and on the erasing conditions of the collected data. As far as the fifth criteria is taken into the analysis, the Court was satisfied since Russian domestic laws "sets out the conditions and procedures for communicating intercepted data containing information about a criminal offence to the prosecuting authorities"[43]. Considering the Russian national legislation from the point of view of the last criteria, the Court found again itself concerned about how Russian legislators had dealt with private data of the citizens: in particular, the Court criticized "the lack of a requirement to destroy immediately any data that is not relevant to the

[41] Case of *Roman Zakharov v. Russia*, cit., para. 248.
[42] Case of *Roman Zakharov v. Russi*a, cit., para. 253.
[43] Ivi.

purpose for which it has been obtained"[44]. Moreover, the Court stressed that no information concerning the storage of the intercepted material after the end of any trial was foreseeable by the citizens making again the Russian domestic law not adequately limpid. Once having established the six Weber criteria, the Court made clear that even if only one of the previously mentioned criteria had not been respected, it would not have allowed any law to be passed by the national legislators.

The Court reasoning around the "*necessary to a democratic society*" wording contained in art. 8 of the ECHR is quite complex as well. On the one hand, in paragraph 232 the Court made clear it acknowledged that "when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security"[45]. On the other hand, the Court clarified that it always exists the risk that secret services could undermine or even destroy democracy while attempting to protect it by violating its fundamental rights: adequate and effective guarantees against abuse must exist.

According to the Court there should exist an independent authority charged to supervise the established restrictive measures in order to always keep the interferences to what is indeed "*necessary to a democratic society*"[46]. On this matter, the Court recognized that the reviewing and supervising operations could come into play at various stages of the surveillance process, including its initiation, execution, and during the conclusive phase. It is clear to the Court from the meaning of secret surveillance itself that during the first two stages, operations must be done without the individual's knowledge. It follows that, since during the first two stages the individual is incapable of seeking an effective remedy against a possible abuse of power, adequate guarantees safeguarding its rights should exist. According to the Court, the only body capable of guaranteeing the correct respect of any individual's rights is a judicial one. The wording used by the Court does not leave any doubt: "it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure"[47]. For which it concerns the third

[44] Case of *Roman Zakharov v. Russia*, cit., para. 255.
[45] Case of *Roman Zakharov v. Russia*, cit., para. 232.
[46] Ivi.
[47] Case of *Roman Zakharov v. Russia*, cit., para. 233.

and final stage of interception, the Strasbourg Court stressed that the issue of providing notification regarding the surveillance measures is closely connected to the effectiveness of legal remedies and, consequently, the presence of robust safeguards against the misuse of monitoring authorities.

Generally, the opportunity for individuals to seek legal recourse through the courts is limited unless they are informed about surveillance measures conducted without their knowledge: this is unlikely to happen since, as previously stated, in the majority of the cases citizens do not even acknowledge they are being intercepted, hence how could they possibly know what methods have been used by monitoring authorities. In such cases, individuals would be able to retrospectively challenge the legality of those measures. Alternatively, individuals who suspect that their communications have been or are being intercepted should have the ability to approach the courts, ensuring that the jurisdiction of the courts is not contingent upon notifying the subject of interception about the occurrence of such interception in their communications[48].

The conclusion of the Court is clear: "Russian legal provisions governing interceptions of communications do not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance, and which is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications"[49]. According to the Court, Order 70 of the Russian Ministry of Communications empowered public authorities of a too broad and not enough clear margin of appreciation: once having established that the provision did not correctly respect the six Weber criteria, the Court concluded that it did not provide sufficient guarantees against a possible abuse of power. In its conclusions, the Court underlined that the mechanism of interception proposed in Order 70 permitted the storage and processing of irrelevant data too: bulk interception of communications, which allows authorities to collect and analyze large quantities of data, not distinguishing between useful and unrelated information, poses significant risks to privacy rights. The Court emphasized the need for clear and precise rules governing the scope and

[48] Case of *Roman Zakharov v. Russia*, cit., para. 234.
[49] Case of *Roman Zakharov v. Russia*, cit., para. 302.

implementation of surveillance measures, as well as effective oversight mechanisms to prevent abuse.

Even if the Court joined unanimously declaring the case admissible and held unanimously that there was an actual violation of art. 8 of the European Convention of Human Rights, at the end of the text of the decision it is possible to identify the annexed Judge Dedov's concurring opinion and the partially dissenting opinion of Judge Ziemele.

Judge Dedov had the same doubts of the Russian Government concerning the admissibility of the case: is it in the Court's competences to examine domestic laws *in abstracto* without basing its reasoning on a concrete case of an applicant being a direct victim of an abuse? According to Judge Dedov, the Court's actions in the merits of Zahkarov v. Russia case could possibly "shift from the actual application of the law to the potential for interference"[50]. Judge Dedov stressed that in the past the Court had already avoided taking important legal decisions by reasoning *in abstracto*: from the *Silver and Others v. the United Kingdom* case of 1983, to the most recent *Sabanchiyeva and Others v. Russia* of 2013. The Judge had serious doubt on why the Court's approach completely changed during the *Zakharov* case. Moreover, the Judge criticized the Court's decision for being "similar to an expert report, but not a judgment" made by the Council of Europe most important Court when dealing with human rights. Expert monitoring bodies' work is to check on the member states' progress in several legal areas and guiding them through non-binding recommendations, while the ECtHR main objective is to rule on the applications alleging possible human rights violations made by individuals or member states: according to the Judge, the separation of powers had not been respected[51].

Judge Ziemele's partially dissenting opinion concerns neither the admissibility of the case nor the merits, but rather focuses on the compensation for the non-pecuniary damage sustained by the applicant: even if worth to be mentioned, Judge Ziemele's partially dissenting opinion will not be closely analyzed since it is not useful for the general framework of this thesis.

[50] Case of *Roman Zakharov v. Russia*, cit., Concurring Opinion of Justice Dedov.
[51] Ivi.

To conclude, it can be stated that the Zakharov case has had a notable influence on how privacy rights and surveillance practices will be understood throughout Europe. On the one hand it strengthened the need for sufficient safeguards, oversight, and remedies in relation to government surveillance activities, but on the other hand, as it will be closely analyzed later, it set the basis for the controversial decision of *Big Brother Watch and Others v. the United Kingdom*. The judgment also played a part in ongoing discussions about finding the right balance between national security and individual privacy, along with the necessity for strong legal frameworks to govern surveillance in the digital era.

1.5 Conclusions

Throughout the first chapter of this thesis, right to privacy and its intricacies have has been disclosed. It has been delved into the complexities of privacy rights, and, by analyzing the principles of proportionality, consent, and accountability on which it rests, it has been emphasized the importance of striking a balance between the legitimate aims of public authorities and individuals' fundamental rights.

Nationally and at the European level, efforts have been made to safeguard the right to privacy through comprehensive legislative frameworks. By taking a closer look to four European cases like Italy, France, Germany, and the UK, differences and similarities within a series of alternative approaches to privacy protection have been observed. Those countries have enacted laws, regulations, and guidelines for the collection, processing, and sharing of personal data, emphasizing the importance of individuals' consent, limited data usage, and robust security measures. Those countries have tried at the same time to comply with the European Directives throughout the years: from the 1996 Directive to the recent General Data Protection Act, those regulations have had the aim to provide a unified framework for data protection, imposing stricter obligations on organizations and member states, empowering individuals with greater control over their data, and establishing more rigorous mechanisms for enforcement and accountability.

In the right to privacy framework context, Article 8 of the European Convention of Human Rights, probably the most important European provision concerning the right has been widely examined. Through a brief digression over the fundamental decisions

taken over the last decades by the European Court of Human Rights, the evolution of the European right to privacy legal landscape has been dissected.

Two landmark cases from the European Court of Justice and the European Court of Human Rights have been closely analyzed, trying to provide a deeper knowledge of the European Union and Council of Europe legal framework which has been built around the right to privacy. In the 2014 ECJ ruling for *Digital Rights Ireland Ltd v. Minister for Communication et al and Kärtner Landesregierung* the Court stroke down a European Directive, the 2006 Data Retention Directive, which interfered with people's privacy. The following year, the 2015 judgment made by the ECtHR in the *Roman Zakharov v. Russia* case, based on the violation of art. 8 of the European Convention of Human Rights, set a clear precedent for future cases concerning this particular fundamental right: acknowledging the *Zakharov* case will be fundamental in order to better understand the judgment of the ECtHR in the context of *Big Brother Watch and Others v. The United Kingdom*.

As technology advances, it will be imperative for legislators, policymakers, and judicial bodies to continuously assess and adapt privacy laws to effectively find a better working balance between privacy and security. Before taking into the account Big Brother Watch case outcomes, which completely revolutionized the approach to this balance, it will be essential to consider the implications of Edward Snowden revelations in the context of privacy rights. His disclosures of 2013 brought to light extensive surveillance programs conducted by intelligent agencies, raising profound concerns regarding privacy infringements and the delicate balance between national security imperatives and individual rights. In the next chapter, by closely examining the revelations on which the Big Brother Watch case is based, the reader will deepen his comprehension of the evolving landscape of privacy in the digital age and bulk interceptions era and explore the far-reaching implications for legal frameworks and the protection of individual rights.

CHAPTER TWO

BULK INTERCEPTIONS AND THE SNOWDEN REVELATIONS

2.1 Introduction

Before closely analyzing the *Big Brother Watch and Others v. the United Kingdom* case, the facts which gave birth to the abovementioned landmark case of the European Court of Human Rights will be extensively examined.

As it has already anticipated in the previous chapter, the Snowden revelations were based on the strong exploitation by some of the most powerful countries in the world, including the United States and the United Kingdom, of several bulk interception programs aimed to search and eradicate possible threats to public security. Throughout the next section of this chapter, the meaning of the expression "bulk interception" will be widely analyzed: in the second paragraph of chapter two, a digression of what bulk interception are, together with a clear differentiation of this first technique from the targeted surveillance operations, will be produced.

In the third paragraph a historical analysis of the facts behind Edward Snowden actions will follow. Dealing with the facts, essential details which surrounded Snowden's revelations will be provided: who is the well-known "whistleblower" and why he decided to publicly reveal sensitive governmental information will be the driving questions of the paragraph.

The fourth paragraph of the chapter will be centered on the subsequent litigation and consequences of the revelations. Journalists, scholars, governmental organizations, and more generally, the public opinion, were deeply divided by Snowden's actions: if on the one hand some argue that Snowden threatened the national security of multiple countries, others, as it will be later investigated, strongly believe that the notorious whistleblower helped the intelligence community to adapt to the new technological era.

Finally, as in the first chapter, the content of the chapter will be resumed, and some conclusions will be drafted.

2.2 Bulk Interceptions and Targeted Surveillance: A Brief Analysis

To begin, in order to better comprehend why Edward Snowden disclosed the world secret surveillance system built up during the first decade of the XXth century, a brief paragraph explaining what targeted and bulk interceptions are, and why this kind of surveillance action could be morally and concretely harmful for the world population, is necessary.

Bulk interception is a complex proceeding. It would be complicated to define or explain the operation as well, but luckily the Grand Chamber of the European Court of Human Rights managed to exemplify the expression.

First of all, the action of intercepting should be examined: as the Court underlined, communications which are produced in the internet domain are carried inside international sub-marine fiber optic cables operated by different internet providers. Each cable may carry several bearers and each communication mat pass through multiple countries, and so multiple bearers before reaching the end of its path.

By clarifying that there was a clear interference with the applicants right to privacy, throughout the reasoning of the *Big Brother Watch v. the United Kingdom* case, the Court recognized that bulk interception conducted by the United Kingdom implied the tapping of several bearers under the Tempora program. By tapping the cables, the British country was able to collect an incredible amount of private information, and with the exploitation of some "selectors", British authorities were able to determine whether collected data was worth to be kept or not. As the Court emphasized, bulk interception operations are a step-by-step procedure where the level of impact on

individuals' privacy rights intensifies as the process advances: in anticipating the extensive analysis of the case which will be produced in the third chapter of the thesis, four stages of bulk interception were recognized. While in the first stage intelligent services start to intercept electronic communications belonging to a large number of citizens, throughout the second stage, various kinds of selectors are employed, including potent ones like email addresses, along with intricate queries, on the stored communication packets and associated communication data. It is only in the third stage that analysts start to examine the collected data, and finally a fourth stage, in which an actual usage of the data gathered in the previous phases happens, could be initiated: it is clear in the mind of the judges of the Court that, in such a process, the degree of the interference increases as the bulk interception progresses within the four aforementioned stages[52].

When dealing with targeted surveillance, it involves the monitoring of specific individuals or groups suspected of engaging in illegal or threatening activities. This approach is focused and tailored, aiming to gather information on selected targets based on credible intelligence and legitimate grounds. It offers several advantages in terms of efficiency, privacy minimization, and adherence to legal frameworks. Advocates of targeted surveillance argue that it provides a more effective means of investigating and preventing specific threats. By concentrating resources on individuals with reasonable suspicion, law enforcement agencies can direct their efforts where they are most likely to yield actionable intelligence, enhancing public safety and national security. This targeted approach allows for the allocation of limited resources to the most relevant areas, increasing the likelihood of successfully identifying and apprehending individuals involved in illegal or dangerous activities[53].

Furthermore, it can be stated that targeted surveillance operates within a publicly accessible legal framework, ensuring proper authorization and oversight: authorities must provide sufficient evidence to justify the surveillance, often requiring warrants or court orders. This legal scrutiny helps to prevent abuse of power and ensures that

[52] Case of *Big Brother Watch and Others v. The United Kingdom*, Judgment of the European Court of Human Rights.
[53] Houston T., *Mass Surveillance and Terrorism: Does PRISM Keep Americans Safer?*, University of Tennessee, 2017.

surveillance activities are carried out within the boundaries of the law, protecting individual rights, and preserving civil liberties.

Notification of surveillance measures to those who are the target of an investigation is probably the one of the most essential characteristics which distinguish targeted surveillance from bulk interceptions from a judicial point of view: it plays a significant role in evaluating the effectiveness of legal remedies and the presence of safeguards against the misuse of surveillance powers. The action of notification, which is not required in bulk interceptions, is closely linked to the effectiveness of legal remedies before the court and, therefore, to the existence of effective safeguards against the abuse of monitoring powers. The European Court of Human Rights established fundamental principles in the *Klass and Others v. Germany* case to balance the state's secret surveillance powers with the rights of targeted individuals, including the rights to be informed about surveillance measures and the ability to seek legal recourse after the termination of such measures. The growing emphasis placed by the ECtHR on the duty to notify individuals about surveillance measures has been once again underlined in the 2012 decision in *Ekimdzhiev and Others v. Bulgaria*[54].

Individuals who are not under suspicion are less likely to be subject to surveillance, reducing the risk of unwarranted privacy infringements. This focused approach helps to strike a balance between security concerns and individual privacy rights. However, critics express concerns about potential abuses and biases in target selection. They highlight the risk of targeting individuals based on flawed or biased intelligence, which could result in the unjust surveillance of innocent individuals. Additionally, some argue that targeted surveillance may have limitations in detecting emerging or unknown threats. By focusing on specific individuals, broader patterns or connections may be overlooked, potentially hindering the ability to identify larger networks or previously unknown threats.

Regarding this last aspect, bulk interceptions nowadays play a fundamental role: indeed, bulk interceptions permit a large-scale, indiscriminate collection of vast amounts of communications data. This technique makes nearly impossible to miss a possible menace to national security since each communication passes under the lens

[54] Turanjanin V., *When does bulk interception of communications violate the right to privacy? The limits of the state's power and the European Court of Human Rights Approach* in *International Cybersecurity Law Review*, 2022, 4, 115-136.

of the governmental entities charged of the investigation, but it obviously carries some negative implications for security and privacy: the majority of the retained and subsequently analyzed communication data is produced by people who are not involved in any suspicious activity[55].

Bulk interception measures are indeed a double-edged weapon. It can be stated that this approach allows intelligence agencies to cast a wide net and gather extensive information, enabling the identification of emerging threats and terrorist activities that might otherwise go unnoticed: the massive datasets collected through bulk interceptions can be subjected to advanced data analysis techniques, such as artificial intelligence and machine learning algorithms, to identify patterns, correlations, and potential risks. However, the indiscriminate nature of bulk interceptions raises significant concerns regarding privacy and data protection: the collection of vast amounts of data on a large scale can lead to a culture of mass surveillance, eroding individual privacy rights. The sheer volume of data collected through bulk interceptions encompasses the communications of countless individuals who are not suspected of any wrongdoing, making the act become not *necessary to a democratic society*. This raises the possibility of surveillance overreach and the potential for the misuse or abuse of collected information. The privacy implications are compounded by the potential for the storage and retention of this data for extended periods, allowing for future analysis or potential misuse. Moreover, the use of advanced technologies for automated data processing and analysis poses additional privacy challenges: the reliance on algorithms and machine learning techniques raises concerns about the accuracy and potential bias in the identification of threats. Moreover, the risk of false positives or misinterpretation of innocent activities may lead to unwarranted intrusion into the private lives of individuals[56].

Balancing the need for effective security measures with the preservation of privacy rights is a complex task. Striking the right balance requires robust legal frameworks, comprehensive oversight mechanisms, and transparent accountability measures. Safeguards should be in place to ensure that the collection, retention, and use of data

[55] Murray D. & Fussey P., *Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data* in *Israel Law Review*, 52(1), 31-60, Cambridge University Press, 2019.
[56] Turanjanin V., *When does bulk interception of communications violate the right to privacy? The limits of the state's power and the European Court of Human Rights Approach*, cit.

obtained through bulk interceptions are strictly necessary, proportionate, and compliant with legal and constitutional principles. The European Court of Human Rights is nowadays working towards this direction in order to provide a well-balanced legal framework, but before *Big Brother Watch and Others v. the United Kingdom* and even before the previously deeply analyzed *Zakharov v. Russia* judgment, the public opinion was not aware about the concrete existence of those intrusive surveillance measures: Snowden revelations opened Pandora's box.

2.3 The Path Towards the Snowden Revelations

On September 11, 2001, four coordinated attacks held by the al Qaeda network were launched against some of the most critical buildings of both the U.S. financial system and decision-making operations: 19 terrorists took control of four civilian planes disguised as American citizens and redirected them towards the two towers of the World Trade Center in New York and the Pentagon, headquarter of the Defense Department of the United States of America, near Washington. The fourth plane, subsequent investigations discovered, was intended to crash onto the White House, but apparently it was taken back by the passengers and crashed in the state of Pennsylvania. The results of the attack were unheard-of: more than three thousand dead, even more injured, and a billionaire economical damage to the country. It has to be stated that these attacks were very much different from any other terrorist attack made in conventional wars: the 19 hijackers, as anticipated, were disguised as civilians, they were not wearing uniforms or carrying weapons openly, and most of all they conducted the attack to the nation by surprise from within the American country boundaries[57].

In the catastrophic aftermath of the 9/11 attacks, President George W. Bush, designated as Commander-in-Chief of the American armed forces by the U.S. Constitution, enacted the so-called Patriot Act. The law signed by the U.S. President drastically expanded the discretionary power of the secret surveillance agencies to permit them to find possible threats to the nation before any other "9/11" would happen. The ability of the President of the United States to overcome any Senate or House of Representatives decision in times of war or in case of serious attacks to the nation has

[57] Yoo, J., *The legality of the national security agency's bulk data surveillance programs* in *Harvard Journal of Law & Public Policy*, 2014, 37(3), 901-930.

always been a useful tool in the hands of the U.S. "First Man", but after the Watergate scandal and the Nixon's abuses of this kind of power, a special court composed by federal district judges, the Foreign Intelligence Surveillance Court (FISC), was established. The creation of this new court, empowered to demand the U.S. government concrete proofs about any man or woman possible relationship with a foreign power or a terrorist group, was part of a fundamental Act enacted by the U.S. Congress in 1978, the Foreign Intelligence Surveillance Act (FISA). The Act in question tried to balance the powers of the President in wartimes and possible criminal behaviors conducted while gathering citizen's private information[58].

The 2001 USA Patriot Act, acronym of *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, essentially improved what was decided with the previous 1978 law passed by the Congress. Three are the main sections of the Act which may be fundamental to comprehend the future Edward Snowden's actions: sections 206, 207, and 215.

In particular, Section 206, also known as the "roving wiretap provision", expanded the government's authority to conduct surveillance on individuals who might be attempting to evade detection by frequently changing communication devices. It allowed law enforcement agencies to start the monitoring of multiple communication devices used by a specific target, such as phones, computers, or other electronic devices with only one permission from the FISC. This provision was designed to adapt to advancements in technology and enable more effective tracking and interception of communications used by suspected terrorists or other criminals.

At the same time, Section 207, the "lone wolf provision", intended to set the duration of the FISA surveillance of non-U.S. persons: it extended the maximum time allowed for surveillance from 90 days to 120 days before a renewed court order was required. This provision aimed to provide investigators with a longer timeframe to gather intelligence on potential threats and streamline the surveillance process for ongoing investigations involving non-U.S. persons. Moreover, the provision allowed secret surveillance agencies to investigate on someone who might be engaged in terrorist activities: no concrete involvement was needed to start an official investigation.

[58] Yoo, J., *The legality of the national security agency's bulk data surveillance programs*, cit.

Finally, Section 215, the most debated Section of the Act known as "business records provision", granted the government the authority to request access to a wide range of business records, including library records, without the need to demonstrate probable cause or notify the individual involved. In other words, to conduct legal terrorist or counterintelligence investigations, intelligence services may apply to the FISA Court for a warrant for the acquisition of "tangible things" that are "relevant" to the investigation at hand without the need of explanation behind the decision to begin the inquiry[59]. This provision faced significant controversy and criticism due to concerns about potential infringements on privacy rights and First Amendment freedoms. It was revised in subsequent legislation, namely the U.S.A. Freedom Act in 2015, to impose stricter requirements for obtaining such records and to enhance transparency and oversight of these surveillance practices[60].

The practices established by the two aforementioned Acts were meant to be functioning exclusively during times of crisis or in the occurrence of serious threats to the nation, but without the acknowledgment of the citizens, U.S. secret services agencies like NSA and CIA, secretly continued to operate under the protective cloak of the FISA and the Patriot Act for years in the search of possible terrorist plots against the United States.

This indiscriminate collection of private data continued until June 2013: in the early months of the same year, a former NSA and CIA agent named Edward Joseph Snowden made contact with some of the most reliable American newspapers, starting from *The Guardian* with the journalist Glenn Greenwald, planning to change the world intelligence forever. In the summer of 2013 Edward Snowden provided a cache of classified documents to several American journals, from the aforementioned *The Guardian*, to *The Daily Mail* and *The Sun*, revealing the details of various surveillance programs and activities carried out by the NSA and its partners. These documents formed the basis for subsequent news articles and reports that exposed the extent of global surveillance operations: the first article, with a title which did not leave any doubts as "*NSA collecting phone records of millions of Verizon customers daily*", was

[59] Arnbak A. & Goldberg, S., *Loopholes for Circumventing the Constitution: Unrestricted Bulk Surveillance on Americans by Collecting Network Traffic Abroad* in *Michigan Telecommunications and Technology Law Review*, 2015, 21(2), 317-362.
[60] Sawyer, S., *Government Bulk Surveillance from 1978-2020: an Ongoing Violation of Citizens Rights* (Doctoral dissertation, Syracuse University), 2020.

indeed published by the Guardian on June 5th[61]. The just mentioned article was based on the first secreted document disclosed by Snowden which stated that Telecom giant Verizon was ordered by the NSA to provide the Federal Bureau of Investigation and the NSA with metadata on millions of American phone conversations using a warrant issued by the Foreign Intelligence Surveillance Court. According to the document Verizon was prohibited from disclosing the order or the request for customer data to the general public[62].

Subsequent articles exposed additional surveillance programs, both domestic and international, conducted by intelligence agencies: according to Snowden disclosures, United States of America's principal surveillance agency, the National Security Agency, co-working with the United Kingdom's Government Communications Headquarters and five other world powers, started several gigantic mass surveillance programs under the protection of the 1978 Foreign Intelligence Surveillance Act and its improved version, the 2001 Patriot Act: the two main programs disclosed by Snowden's revelations were Prism and Tempora of which the primary purpose was to retrieve data from Internet cables and to intercept it while it was in transit though the installation of interceptors on the massive fiber-optic cables that connected the various hubs of the Internet[63].

A key aspect of the Prism program was the NSA collaboration with major technology companies. Under Prism, the NSA allegedly had direct access to the servers of prominent companies such as Microsoft, Google, Apple, Facebook, and others. This arrangement allowed the NSA to extract a wide range of user data, including emails, chat logs, photos, videos, documents, and other forms of digital communication. The program's direct access to these companies raised concerns about the extent of corporate cooperation, the potential for warrantless surveillance, and the erosion of privacy rights. Prism operated under the legal authority of Section 702 of the Foreign Intelligence Surveillance Act. It required court-approved orders from the secretive Foreign Intelligence Surveillance Court to target specific individuals or groups for

[61] Greenwald G., *NSA collecting phone records of millions of Verizon customers daily*, 2013 [Online], Available at: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.
[62] Lyon D., *Surveillance, Snowden, and Big Data: Capacities, consequences, critique* in *Big Data & Society*, 2014, 1(2).
[63] Bauman Z., Bigo D., Esteves P., Guild E., Jabri V., Lyon D. & Walker R. B. J., *After Snowden: Rethinking the Impact of Surveillance* in *International Political Sociology*, 2014, 8(2), 121–144.

surveillance. While the program primarily focused on gathering foreign intelligence and targeting non-U.S. citizens outside the United States, there were reports of incidental collection of communications involving U.S. citizens. The information collected through the program underwent extensive analysis and processing by the NSA and other intelligence agencies. Advanced search algorithms and data mining techniques were employed to search for keywords, patterns, and connections to identify potential threats. The program also facilitated information sharing with other agencies, both domestically and internationally, through established intelligence-sharing partnerships[64].

On June 21st of 2013, The Guardian published another article revealing the Tempora program conducted by the UK's Government Communications Headquarters. This program involved the installation of data interceptors on fiber-optic cables carrying Internet data within and outside the UK, including transatlantic connections between the US and Europe. As a significant landing point for transatlantic cables, the UK managed to intercept a substantial amount of global communications traffic. According to the report, the volume of intercepted data through Tempora was described as massive, and it was directed from the cable probes to GCHQ's monitoring stations, where it was stored using the agency's Internet buffers. GCHQ stored the colossal amount of internet data obtained through Tempora for varying durations: up to 72 hours for the actual content and up to thirty days for metadata. The data was then searched using keywords, agreed upon by both GCHQ and the North American NSA, totaling approximately 40,000 selector pointers. Identified signals underwent further examination by operatives, who analyzed the respective communications[65].

It should be clear that Snowden revelations did not focus solely on the United States intelligent agencies: he made sure that even operations carried out by the GCHQ and the U.S. alliance with the so-called "Five Eyes" came to light. As he underlined during the disclosures, the activities of both the NSA and GCHQ mutually benefited each other. A significant portion of data obtained through the PRISM program was transferred to GCHQ servers. Moreover, Tempora contributed to the NSA's work,

[64] Houston T., *Mass Surveillance and Terrorism: Does PRISM Keep Americans Safer?*, cit.
[65] Georgieva, I., *The right to privacy under fire foreign surveillance under the NSA and the GCHQ and its compatibility with art. 17 ICCPR and art. 8 ECHR*. in *Utrecht Journal of International and European Law*, 2015, 31(80), 104-130.

permitting the American agency to have an even wider control over the world possible threats.

It is worth noting that Snowden's decision to publish the documents was not without personal risks: after the disclosures, well aware that he would likely face legal repercussions for his actions, Snowden left the United States and traveled to Hong Kong where he continued to work with journalists disclosing more information. As the US government sought his extradition, Snowden sought legal advice and explored options for seeking asylum to protect himself from prosecution. After attempting to reach Latin America, Snowden's travel plans were disrupted, and he ended up stranded in Moscow's Sheremetyevo Airport. Russian authorities granted him temporary asylum, allowing him to remain in Russia, where he took the Russian citizenship and currently resides[66].

The world's most famous whistleblower did not reveal his identity immediately. As stated before, the very first article from *The Guardian* disclosing the NSA operations which involved the telephone company Verizon, was published on the 5th of June while the former NSA contractor was already in Hong Kong. In the region, where he met again with the journalist from *The Guardian*, Glenn Greenwald, he agreed on the publication of a new article: one week after he shocked the world, on the 11th of June, the secret whistleblower found publicly a name and a face. In the article, titled "*Edward Snowden: the whistleblower behind the NSA surveillance revelations*", *The Guardian* presented the man behind the facts and the reasons behind his actions. Snowden was not an anarchist trying to undermine the established order. On the contrary, as it can be witnessed from the article, he decided to give up his former life because his principles were stronger than his need for a career and money: "My sole motive is to inform the public as to that which is done in their name and that which is done against them […]. I'm willing to sacrifice [my former life] because I can't in good conscience allow the US government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building"[67].

[66] MacAskill E., *"No regrets", says Edward Snowden, after 10 years in exile*, 2023 [Online], Available at: https://www.theguardian.com/us-news/2023/jun/08/no-regrets-says-edward-snowden-after-10-years-in-exile.

[67] Greenwald G., *Edward Snowden: the whistleblower behind the NSA surveillance revelations*, 2013 [Online], Available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

By highlighting and exposing the extensive surveillance activities conducted by intelligence agencies, Snowden aimed to bring attention to what he believed was a violation of individual privacy rights and a breach of public trust. Snowden firmly believed that individuals should have the right to know the extent to which their private communications and activities were being monitored by governments: as he declared to The Guardian "I carefully evaluated every single document I disclosed to ensure that each was legitimately in the public interest. There are all sorts of documents that would have made a big impact that I didn't turn over, because harming people isn't my goal. Transparency is"[68].

Moreover, once arrived in Moscow, Snowden managed to release a statement to Human Rights Groups at Moscow's Sheremetyevo Airport. The statement leaves no room for doubt about his motives for acting as a "civil disobedient": "I believe in the principle declared at Nuremberg in 1945: Individuals have international duties which transcend the national obligations of obedience. Therefore, individual citizens have the duty to violate domestic laws to prevent crimes against peace and humanity from occurring. […] I did what I believed right and began a campaign to correct this wrongdoing. […] If you have any questions, I will answer what I can"[69].

In sum, in just six days, with just a few documents disclosed compared to the vast amount of secret information he was able to bring with him to Hong Kong, Snowden triggered a political controversy more intense than the one caused some years before by Julian Assange and the WikiLeaks crisis, leaving the world intelligence, the United States, and its allies with the consequences of his actions.

2.4 Subsequent Litigation

Snowden revelations paved the way to different scenarios. First of all, the world's major powers were called for the first time to explain to their citizens why they operated such intrusive secret surveillance programs and most of all, if those programs served their purpose: did they manage to increase citizens' security or in the end they violated privacy rights without bringing concrete results? Secondly, since Snowden completely

[68] Ibidem.
[69] Scheuerman W. E., Whistleblowing as civil disobedience: The case of Edward Snowden in Philosophy & Social Criticism, 2014, 40(7), 609-628.

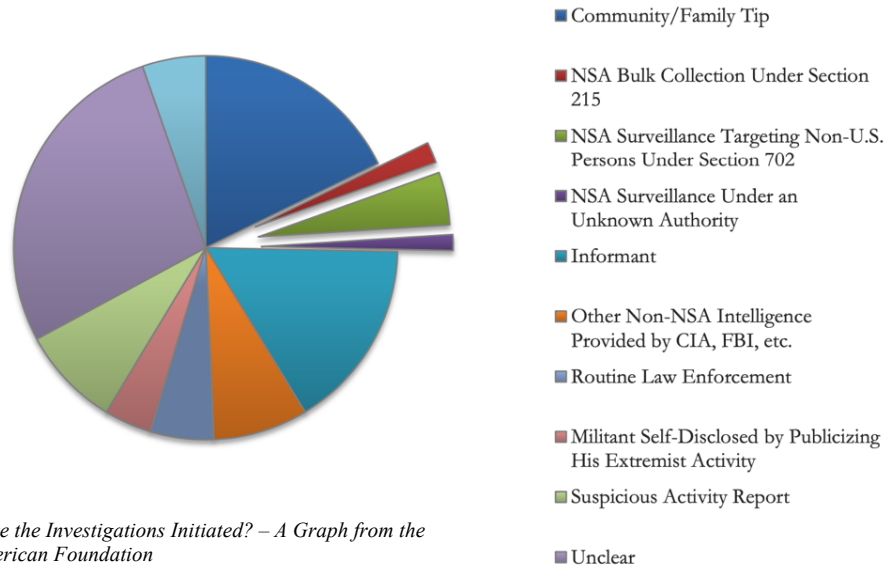
destroyed the intelligence of several countries in the world, governments had to initiate a process of which the ultimate aim was to rebuild their intelligence network trying to comply with people's needs of transparency and accountability. Finally, although conventions had been signed and international treaties had been ratified, governments had clearly showed that they could not guarantee the respect of fundamental human rights anymore: the legal framework concerning the right to privacy had to be renewed in the perspective of a an ever more interconnected and technological world.

Immediately after the first disclosures, some both U.S. and UK politicians released so e statements affirming that they were not aware of the broadness of NSA and GCHQ's bulk data-collection programs, raising questions about whether these organizations were sufficiently informing their governments about their operations[70]. Two weeks after the publishing of the first article revealing the existence of a very intrusive world surveillance network, while visiting Berlin, former President of the United States Barack Obama overturned the claims stating that "at least 50 threats that have been averted because of this information not just in the United States, but, in some cases, threats here in Germany. So, lives have been saved"[71]. Two other statements from former NSA Director Gen. Keith Alexander and Representative Mike Rogers justified secret operations conducted by NSA and its allies as fundamental for citizens' security all over the world. The former, testifying before the Congress, declared that "the information gathered from these programs provided the U.S. government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world"[72], while the latter, Chairman of the House Permanent Select Committee on Intelligence, said on the House floor in July that "54 times NSA programs stopped and thwarted terrorist attacks both here and in Europe saving real lives"[73].

The reliability of these statements can be considered somewhat questionable. New investigations carried out by *The New America Foundation* brought up to light that, since the 9/11 events and the subsequent approval of the 2001 Patriot Act, over 200

[70] Inkster N., *The Snowden revelations: Myths and misapprehensions* in *Survival Global Politics and Strategy*, 2014, 56(1), 51-60.
[71] Calmes J., *Obama Says Surveillance Helped in Case in Germany*, 2013 [Online], Available at: https://www.nytimes.com/2013/06/20/world/europe/obama-in-germany.html.
[72] Disclosure of National Security Agency Surveillance Programs: Hearing before the H. Perm. Select Comm. on Intelligence, 113th Cong., statement of Gen. Keith Alexander, Director of NSA, 2013.
[73] Congressional Record, House of Representatives, 113th Cong., 2013.

terrorist cases were initiated in the American country and just a few of those terrorist plots were identified thanks to the bulk collection of data operated by the National Security Agency, the UK's Government Communications Headquarters and their allies all over the world. More precisely, of the 225 cases of crimes committed by U.S. citizens within the U.S. borders or abroad, 4 of them were identified under Section 215 of the Patriot Act. Moreover, according to further declarations from Gen. Keith Alexander obtained after a tough questioning from Senator Patrick Leahy during a Senate Judiciary Committee hearing in October, only one terrorist activity was prevented thanks to the bulk surveillance activities under Section 215[74]. Below, the graph with the conclusions obtained by *The New American Foundation* with its related database.



How were the Investigations Initiated? – A Graph from the New American Foundation

Key Method	# of Cases	% of Total Cases
Community/Family Tip	40	17.8
NSA Bulk Collection Under Section 215	4	1.8
NSA Surveillance Targeting Non-U.S. Persons Under Section 702	10	4.4
NSA Surveillance Under an Unknown Authority	3	1.3
Informant	36	16.0
Other Non-NSA Intelligence Provided by CIA, FBI, etc.	18	8.0
Routine Law Enforcement	12	5.3
Militant Self-Disclosed by Publicizing His Extremist Activity	9	4.0
Suspicious Activity Report	19	8.4
Unclear	62	27.6
Plot Not Prevented Prior to Incident	12	5.3

Full Database – New American Foundation

[74] Bergen P., Sterman D., Schneider E., & Cahall B., *Do NSA's Bulk Surveillance Programs Stop Terrorists?*, New America, 2014.

The database shows a discrepancy between comments made by government officials justifying the bulk phone metadata programs of the NSA and its allies as essential to citizens' security and how it has actually been used. Officials have cited saving time on investigations as one of the reasons why mass acquisition of American phone information is required. But the evidence clearly does not support the government's claims of efficiency[75].

For which it concerns the rebuilding process which characterized the world intelligent agencies in the aftermath of Snowden revelations, a new "forced transparency" of the intelligence services started spreading across the world: for the first time ever intelligence agencies had to justify their actions before the people. It is fundamental to state that if on the one hand Snowden revelations initially undermined the stability of the world intelligence and most of all of the NSA and the GCHQ, generating a strong negative sentiment of the public opinion towards the surveillance programs adopted up to that time[76], on the other hand, as Harvard Professor, former Assistant Attorney General of the United States of America Jack Goldsmith stated, "the sky did not fall". In an article published in 2016 on Lawfare, Professor Goldsmith stated that the intelligence community, and in particular the National Security Agency, managed to emerge from the Snowden crisis in an apparent good shape: as example, in the U.S. new oversight institutions including President's Review Group and most of all Privacy and Civil Liberties Oversight Board were established. Provisions limiting the collection of data from non-U.S. citizens like the Presidential Policy Directive 28 were enacted too. Snowden revelations forced the GCHQ to confront the fact that its surveillance methods and capabilities were now publicly known too: exploring alternative surveillance methods, adopting more sophisticated encryption technologies, and diversifying their approaches to stay ahead of potential adversaries were some of the main objectives for UK's intelligent services during the post-Snowden era. Additionally, the GCHQ sought to enhance engagement with oversight bodies and independent reviewers. They established closer relationships with the Investigatory Powers Commissioner's Office (IPCO), which provides independent oversight of the

[75] Ibidem.
[76] Reddick C. G., Chatfield A. T. & Jaramillo, P. A., *Public opinion on National Security Agency surveillance programs: A multi-method approach* in *Government Information Quarterly*, 2015, 32(2), 129-141.

UK's intelligence agencies. By subjecting their actions to external scrutiny, the GCHQ aimed to start their rebuilding process by ensuring that their activities were accountable, lawful, and proportionate. Since the intelligence community had no prior experience in explaining itself, it was first a tedious and even confusing procedure, but it turned out that transparency had a lot of advantages: although the first reaction of the world public was a comprehensible feeling of betrayal carried out by the institutions, enough was disclosed by the authorities to make people comprehend the value of the work of agencies permitting agencies like GCHQ or NSA to regain public confidence, address privacy concerns, and demonstrate a commitment to responsible and accountable intelligence operations[77].

Finally, for which it concerns the right to privacy legal framework, the last theatre on which the Snowden revelations had a great impact, the actions of the whistleblower provoked serious consequences. Snowden had showed that the right to privacy was not respected concretely. There is no doubt that European lawmakers were already working towards an upgrade of the legal landscape of this right: the reader has already had the possibility to closely examine the *Zahkarov v. Russia* case, where efforts from the European Court of Human Rights to find a balance between the right to privacy and ever more technological methods of collecting and analyzing private data were made. But Snowden's disclosures about the existence of the Prism and Tempora programs brought several companies, organizations, and individuals to file a suit against the United Kingdom: the resulting *Big Brother Watch and Others v. The United Kingdom* case, which has recently led to a renewal of the legal framework around the right to privacy, will be closely discussed in the next chapter.

2.5 Conclusions

Throughout the second chapter of this thesis, it has been tried to provide a wider knowledge about the facts and information on which the *Big Brother Watch and Others v. The United Kingdom* case relies.

[77] J. Goldsmith, *Three Years Later: How Snowden Helped the U.S. Intelligence Community*, 2016 [Online]. Available at: https://www.lawfareblog.com/three-years-later-how-snowden-helped-us-intelligence-community.

After a brief introductive paragraph, the key distinctions between bulk interceptions and targeted surveillance, shedding light on the covert methods employed by intelligence agencies to combat potential threats to democracies, have been examined. Through a brief analysis of these techniques, the main differences which characterize the two principal tools in the hands of the intelligent services have been provided: from the large-scale and intrusive bulk interceptions, where millions of people may be involved during the data collection phase without their acknowledgement, to the targeted surveillance methods, where an initial clear suspicion may give rise to an interception of specific individuals or group after a prior authorization of judicial bodies.

Through a historical digression into the Snowden revelations, the pivotal moments that exposed the extent of bulk interceptions as the primary tools used by intelligence agencies have been addressed: from the aftermath of the catastrophic 9/11 events and the subsequent intelligent services enforcement, to the actions of the world most notorious whistleblower and the reasons which prompted him disclosing secreted information.

The consequences of these revelations were far-reaching and multi-faceted, impacting the agencies' relationship with the public, provoking a rebuilding process within the intelligence community, and having severe legal implications. Snowden revelations marked a turning point in the public's perception of intelligence agencies' activities. As the veil of secrecy was lifted, agencies faced the daunting task of justifying their actions to a skeptical public. The revelation of the scale and scope of mass surveillance programs left citizens questioning the balance between security and privacy, demanding greater transparency and accountability from their governments. Governments and agencies found themselves engaged in a battle of persuasion, attempting to convince the people of the necessity and effectiveness of their surveillance efforts: the analysis made in the fourth paragraph of the chapter has showed how, at least initially, governments were not able to justify the existence of such intrusive programs.

In the same paragraph, it has been shown how the disclosures made by Snowden triggered a complete restructuring of the intelligence community. The once-untouchable realm of covert operations and intelligence gathering was forced to adapt

to the new reality of heightened public scrutiny. The agencies had to navigate the delicate process of rebuilding public trust and reevaluating their methods to ensure they aligned with the evolving standards of privacy and human rights. This process was not without its challenges, as the revelations shook the foundations of the intelligence community and necessitated significant reforms in policies and practices.

From a legal standpoint, the impact of the Snowden revelations was also substantial. The case of *Big Brother Watch and Others v. The United Kingdom*, as it will be closely discussed in the following and final chapter of this thesis, stands out as a landmark legal battle in which the legality of mass surveillance practices was brought into question. The revelations prompted legal challenges and debates over the extent to which bulk interceptions violated fundamental rights and breached international human rights standards. This case, among others, led to an increased scrutiny of intelligence agencies' activities and highlighted the need for robust legal frameworks to govern surveillance practices in the digital age.

In conclusion, the revelations brought forth by Edward Snowden had far-reaching consequences for the intelligence community, the relationship between agencies and the public, and the legal landscape surrounding mass surveillance. They forced agencies to justify their actions, sparked a process of rebuilding and reform within the intelligence community, and triggered legal debates and challenges. The final chapter of this thesis will focus on this last point through a deeper analysis of the aforementioned *Big Brother Watch* case, and with a closer look to the case of *Centrum för Rättvisa v. Sweden*, the most recent landmark judgment of the ECtHR which revolves around the right to privacy.

CHAPTER THREE

BULK INTERCEPTIONS BEFORE THE ECTHR: THE BIG BROTHER WATCH AND CENTRUM FÖR RÄTTVISA JUDGMENTS

3.1 Introduction

In the digital age, the right to privacy has become a pivotal concern, as technological advancements have enabled extensive surveillance capabilities by governments and other entities. As, so far, it has been delved deeper into the intricacies of privacy rights and their application in the context of intelligence gathering, after this brief introductory paragraph, the second paragraph of this final chapter aims to explore and analyze the landmark case of *Big Brother Watch and Others v. the United Kingdom*. Throughout the paragraph, the facts behind the applications and the key arguments presented by the parties involved, the court's findings, the final decision, and the broader implications of this ruling on privacy rights will be closely examined.

The third paragraph of this chapter will delve into one of the main aspects that emerged from the Big Brother Watch case: the concept of extraterritoriality of the right to privacy. It will be critically analyzed whether Article 8 of the European Convention on Human Rights, which guarantees the right to respect for private and family life, is universally applicable beyond national borders. The implications of extraterritoriality on surveillance practices, data protection, and individual rights will be examined to understand its impact on global privacy norms and regulations.

Although, anticipating the final judgment, the justices of the ECtHR held unanimously that there has been a violation of Art. 8 of the Convention, several judges provided some dissenting and concurring opinions. The fourth paragraph will focus on those diverse opinions expressed by the justices in the *Big Brother Watch* case. By examining both the dissenting and concurring opinions expressed by judges Lemmens, Vehabović, Bošniak, Ranzoni, and Pinto de Albuquerque annexed at the end of the ruling, the author aims to gain insights into the judicial reasoning behind the decision and the different perspectives within the ECtHR on privacy rights: understanding these varying viewpoints, not only will shed light on the complexities surrounding the interpretation and application of privacy protections in the digital age, but it will also give the reader the opportunity to better comprehend the direction towards which the European legal framework of the right to privacy is currently going.

In the fifth paragraph, the *Centrum för Rättvisa* case, the most recent judgment by the European Court of Human Rights concerning the right to privacy will be briefly analyzed. By comparing this recent ruling with the *Big Brother Watch* case, any potential shift or development in the court's approach to privacy rights and their extraterritorial implications will be identified. This analysis will contribute to the understanding of how privacy rights are evolving in response to the rapidly changing technological landscape and how the Big Brother judgement has influenced the following decisions.

In the sixth paragraph of this chapter, conclusions based on the findings and analyses presented in the preceding sections will be drawn. This part will summarize the key insights gained from the *Big Brother Watch* and *Centrum för Rättvisa* cases. By synthesizing this information, a comprehensive understanding of the complexities surrounding privacy rights and their relevance in the digital age will be provided: reflections on the broader implications of these cases for the protection of individual liberties and the future of privacy rights in the context of intelligence gathering and surveillance practices will be offered.

Finally, a concluding paragraph providing a brief summary of the information and the content presented throughout the chapter will be drafted.

3.2 Big Brother Watch and Others v. the United Kingdom: Applications, Case and Final Judgment

3.2.1 *The applications*

It has already deeply analyzed how Snowden opened the Pandora's box of secret surveillance measures around the world: *Big Brother Watch and Others v. the United Kingdom* is probably the most important consequence from a legal point of view. Indeed, following the Snowden revelations, three applications were presented to the Strasbourg Court from both journalists and NGOs which "all believed that due to the nature of their activities, their electronic communications were likely to have either been intercepted by the United Kingdom intelligence services; obtained by the United Kingdom intelligence services after being intercepted by foreign governments; and/or obtained by the United Kingdom authorities from communications service providers"[78]. The applications were all made with the firm belief that the UK's surveillance programs disclosed by Edward Snowden which operated under the *Regulation of Investigatory Powers Act*, also known as RIPA, violated several provisions of the European Convention of Human Rights.

Dated the year 2000, the Act in question was enacted by the English government in order to address the significant challenges posed by the recent advancements in technology trying to reach a perfect balance between national security interests and the protection of individual privacy rights: providing a legal framework for conducting electronic surveillance while safeguarding the nation against evolving threats such as terrorism and cybercrime were the key driving objectives behind the decision of enacting the Act. Under RIPA, law enforcement and intelligence agencies had the authority to intercept communications, such as phone calls, emails, and internet communications, under specific circumstances. To obtain authorization for such interceptions, the Secretary of State or designated officials must be satisfied that those were proportionate and necessary for purposes such as national security, preventing or detecting crime, or safeguarding the economic well-being of the UK The Act also allowed authorities to access communications data, which includes information about the communication, such as phone numbers, email addresses, and location data. Access

[78] Case of *Big Brother Watch and Others v. The United Kingdom*, Judgment of the European Court of Human Rights, para. 13.

to communications data was granted to various public bodies for specific purposes, including those related to national security and crime prevention.

To go deeper into the examination of the provision which brought to the three applications, the RIP Act was divided into five parts: the acquisition, disclosure, and interception of communications data were the main topics regulated in the first part. The Act's second part dealt with covert human intelligence sources. This provision of the Act provided a legal foundation for the authorization and use of covert surveillance, agents, informants, and undercover officers by security and intelligence agencies, law enforcement, and other public bodies. The third part of the RIPA dealt with the state and possibly other public and private entities' examination of encrypted electronic data. According to Section three, the Secretary of State and other senior authorities had the power to demand the disclosure of protected or encrypted material. Part IV of the legislation ensured the presence of an impartial judicial oversight concerning the granted powers by establishing the Investigatory Powers Tribunal (IPT) as a mechanism to address complaints related to the unauthorized use of these powers. Furthermore, the Act granted authority to the Secretary of State to issue Codes of Practice that govern the utilization of these powers. Finally, the fifth and last part concerned supplementary matters as minor revisions of older provisions in order to make them comply with the new legislation[79].

Between 2013 and 2015, heavily relying on Edward Snowden disclosures, the applicants complained a possible violation of rights to privacy and freedom of expression, both of them protected under Articles 8 and 10 of the ECHR, before the aforementioned IPT. Three different hearings were made: the domestic tribunal yet recognizing that some data collected from Amnesty International had been stored for an amount of time longer than permitted by the same RIPA legislation and finding that the procedure for the selection of the data set by the same legislative provision had not been followed correctly, was substantially satisfied from the GCHQ proceedings[80].

Once having exhausted all the domestic proceedings, one of the main admissibility criteria listed in Art. 35 of the Convention in order to bring a complaint before the

[79] Reid A. & Reyder N., *For Whose Eyes Only? A Critique of the United Kingdom's Regulation of Investigatory Powers Act 2000* in *Information & Communications Technology Law*, 2001, 10(2), 179-201.
[80] Case of *Big Brother Watch and Others v. The United Kingdom*, cit., para. 31-60.

ECtHR, the applicants decided to the lawsuit before the Strasbourg Court. In 2017 the different applications were joined by a Chamber of First Section which, analyzing the facts behind the application, on the one hand declared admissible the complaints made by the applicants, and on the other hand it recognized a violation of Articles 8 and 10 of the European Convention of Human Rights in respect of both section 8 and Chapter II of the RIP Act. In 2019 the composition of the Grand Chamber was determined in order to work towards the resolution of the case[81].

3.2.2 *The case: the Chamber prior's judgment*

It must be noted that the Grand Chamber decision, which will be analyzed later in the following subparagraph, is a direct consequence of the work of the ECtHR's Chamber prior judgment: the work of the Chamber in the Big Brother Watch case involved examining the merits of the application, well exhausted in the previous subparagraph, assessing alleged violations of Convention rights, and delivering a preliminary judgment. As anticipated in the previous subparagraph, the main issues analyzed by the Court's Chamber revolved around three main parts of the 2000 Regulation of Investigatory Powers Act: section 8, of which the fourth paragraph concerned the bulk interception of communications, Chapter II, which main aim was to regulate the obtaining of communications data from communication service providers, and intelligence-sharing arrangements set in the 2000 provision. A violation of Art. 8 of the Convention was indeed identified by the Chamber: in particular, a breach was found referring to Section 8 and Chapter II, while the intelligent-sharing arrangements with foreign governments or other intelligent agencies were found to comply with the Convention[82].

With its preliminary judgment, later confirmed by the Grand Chamber, the Chamber expressed its firm idea over bulk interceptions: implementation of bulk surveillance programs is considered an interference but not an automatic violation of Article 8. The Chamber asserts that it falls within the State's discretion to operate such programs to identify potential national security threats: as it is stated in paragraph 314 of the final

[81] Ivi, para. 4-10.
[82] Watt E., *Much Ado About Mass Surveillance – the ECtHR Grand Chamber 'Opens the Gates of an Electronic "Big Brother" in Europe' in Big Brother Watch v UK*, cit.

judgment's text "the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation"[83]. Additionally, the Chamber recognized the value of bulk interception "in achieving the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime"[84]. However, a breach of Article 8 can occur if the operation of these programs fails to adhere to prescribed safeguards and lacks sufficient oversight mechanisms. In other words, while the existence of bulk surveillance programs is acceptable, their compliance with safeguards and oversight is crucial to avoid violating individuals' privacy rights under Article 8.

Pursuing in the examination of its preliminary judgment, the Chamber focused on the principles of "*reasonable suspicion*" and "*subsequent notification*" introduced in the *Zakharov* case when dealing with targeted surveillance as the applicants claimed that such principle should be applied to bulk interceptions too. In paragraph 317 it is well investigated the reason why, according to the Court, the application of those principles to bulk interceptions is not possible. Bulk interception involves the collection and analysis of a vast amount of data from a large number of people. Unlike targeted surveillance, where authorities have specific suspects in mind, bulk interception casts a wide net, capturing communications and data from numerous individuals, most of whom are not suspected of any wrongdoing. This makes it practically impossible to apply the "*reasonable suspicion*" principle to each individual affected. Additionally, in bulk interception operations, the specific targets are not pre-identified: the surveillance is often conducted to gather intelligence on potential threats or to identify unknown targets, rather than monitoring specific individuals or groups suspected of criminal activity. As a result, the "*reasonable suspicion*" principle, which requires a targeted approach, becomes challenging to implement. Finally, for which it concerns the subsequent notification to each individual whose data has been intercepted, the Court stated that this was simply not practical or feasible in the context of bulk interception: since mass surveillance operations involve large-scale data collection, notifying each individual could compromise ongoing investigations or intelligence-gathering efforts[85].

[83] Case of *Big Brother Watch and Others v. The United Kingdom*, cit., para. 314
[84] Ivi, para. 386.
[85] Ivi, para. 317.

What is clear from the judgment of the Chamber of First Section of the European Court of Human Rights is that mass surveillance is an essential tool in the hand of the governments in order to identify and subsequently strike down possible threats to national security: once having established that governments enjoy a wide margin of appreciation in choosing when starting a mass surveillance operation, and once having stated that, in the case of existence of adequate safeguards and oversight institutions, bulk interceptions are to be considered feasible tools in the hand of intelligent agencies, the rest of the ruling was left in the hands of the Grand Chamber of the ECtHR. Whether the Grand Chamber would adhere to its existing approach or shift course, aligning its thinking with the one used in the *Zakharov v. Russia* case on domestic surveillance, remained a pressing question for civil society, privacy advocates, and academics. The potential outcome of this decision could result in a heightened level of protection concerning the mass acquisition of foreign communications.

3.2.3 *The case: the Grand Chamber's final decision*

There should be no surprise in finding that the Grand Chamber largely confirmed what the Court's First Section had priorly decided: as it is stated in paragraph 323, the global Internet's technological advancements have led to a significant increase in communication volumes, and alongside this, the Court had recognized that Contracting States and their citizens are continuously confronted with a multitude of threats, including global terrorism, drug trafficking, human trafficking, and the sexual exploitation of children. These dangers often originate from international networks of hostile actors who exploit sophisticated technology to communicate without detection. Furthermore, access to such technology allows both State and non-State adversaries to disrupt digital infrastructure and democratic processes through cyberattacks, a digital domain-exclusive national security concern, that necessitates detection and investigation within that realm. Consequently, the Court's Grand Chamber had to evaluate Contracting States' bulk interception operations as a valuable asset for identifying emerging digital threats[86]. As underlined by the Court, the Venice Commission too, in 2015, had expressed over the subject of bulk interceptions, considering them of vital importance to possibly identify unknown threats to national

[86] Ivi, para. 323.

security[87]. Given that, the Court ultimately confirmed that the mere usage of bulk interception methods did not constitute a violation of the rights listed in Art. 8.

If on the one hand the Grand Chamber limited itself to confirming what was previously established by the Chamber of First Section, on the other hand it produced new, fundamental jurisprudence: the Court's objective was to set out up to date, essential safeguards to reduce the risk of bulk interception powers being abused by intelligence agencies. In order to do that, the Court firstly made a clear differentiation between targeted surveillance and bulk interception: While targeted interception is commonly used by respondent States for investigating crime, bulk interception is more frequently employed by Council of Europe member States for foreign intelligence gathering, early detection and investigation of cyberattacks, counterespionage, and counterterrorism. Even if bulk interceptions are not meant to target specific individuals, it is obvious in the mind of the justices of the Court that they can be used for this purpose: the application of strong selectors to what was intercepted during the bulk phase make the citizens object of the previous collection of data "targeted"[88]. Once having established the interconnection between bulk interceptions and targeted surveillance methods, the Court underlined the necessity to fit the already existing six safeguards set out in *Zakharov v. Russia* of 2013, to bulk interceptions: it is fundamental to adapt the Weber criteria, previously developed by the Court to be referred to targeted surveillance techniques, to bulk methods of collection[89]. Between paragraphs from 348 to 364 the Court focused on updating the Weber criteria in order to shrink possible abuses of bulk interception methods.

According to the Court, the differences between targeted and bulk interceptions make some of the Weber criteria not easily applicable to bulk interception cases. The "*reasonable suspicion*" principle was already deemed to be considered unsuitable in the context of bulk interception operations by the Chamber in its prior judgment as those kinds of techniques are meant to forestall a threat: the "*reasonable suspicion*" concept has been developed to justify the investigation of a specific target which is

[87] European Commission for Democracy Through Law (Venice Commission), *Report on the Democratic Oversight of Signals Intelligence Agencies*, Strasbourg, 15 December 2015.
[88] Case of *Big Brother Watch and Others v. The United Kingdom*, cit., para. 344-346.
[89] Watt E., *Much Ado About Mass Surveillance – the ECtHR Grand Chamber 'Opens the Gates of an Electronic "Big Brother" in Europe' in Big Brother Watch v UK*, cit.

believed could commit or has committed a crime, subsequently only suitable to the targeted surveillance programs.

Two other requirements which clearly cannot be convenient to bulk interception according to the Court are the need for the domestic law to clearly set the nature of the offences which could may give rise to an interception order, and the obligation to specify which are the categories of people possibly being subject of an interception: as a perpetual, mass research of possible threats to national security, the two aforementioned requirements result almost impossible to apply to bulk interception regimes[90]. In spite of this, "the Court considers it imperative that when a State is operating such a regime, domestic law should contain detailed rules on when the authorities may resort to such measures. In particular, domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorized and the circumstances in which an individual's communications might be intercepted"[91].

At the same time, former safeguards were considered equally applicable to mass interception regimes: setting out in domestic law the limits on the interception's duration, the procedures to be followed during the examination, usage, and storing of the data collected, the precautions to be taken for communicating the data to other parties, and the circumstances when the obtained material must be erased or destroyed, is identically relevant for both targeted and bulk interception regimes.

It should now be clear that it was not the Court's intention to change the "legal climate" of the now well-established bulk interception regimes' policies aimed at identifying threats to national security. The Court already had extensively reiterated the existence of a state margin of appreciation in this matter and, to some extent, even expressed appreciation for such trend: to recall what underlined in the previous pages, the Court stated that "it is clear that bulk interception is a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime"[92]. It was no longer the legitimacy as such of mass surveillance policies, which was already widely acknowledged by the Court both from the *Zakharov v. Russia* outcomes and from the very first paragraphs of this judgment, the main concern of the Court. Instead, the focus lied on the specific methods,

[90] Case of *Big Brother Watch and Others v. The United Kingdom*, cit., para. 348.
[91] Ibidem.
[92] Ivi, para. 386.

requirements, and assurances outlined by national laws during the practical execution of these policies[93]. In this regard, the Court limited the discretion given to states to reduce the potential for misuse of power, requiring bulk interception programs to adhere to updated safeguards that include the former six Weber criteria revised, along with additional provisions suitable for contemporary circumstances. The newly introduced eight comprehensive and updated safeguards were the following.

Firstly, the Court emphasized the need for well-defined and explicit grounds on which bulk interception may be authorized. This means that interception measures must be limited to specific and legitimate purposes, such as addressing national security threats or serious crimes, and not extended to arbitrary or indiscriminate surveillance. The circumstances under which an individual's communications may be intercepted were closely examined too in the second safeguard settled by the Grand Chamber: "the grounds on which bulk interception may be authorized and the circumstances in which an individual's communications may be intercepted must be defined in the domestic legal framework".

Thirdly, the Court highlighted the significance of a robust and rigorous authorization procedure for bulk interception measures. This implies that competent and independent authorities should be involved in granting authorization, and such authorizations should be subject to proper scrutiny and oversight to prevent potential abuses of power.

Furthermore, the Court underscored the necessity for clear procedures in selecting, examining, and using the intercepted material. This means that interception measures should focus on collecting relevant and necessary data, with stringent measures in place to prevent indiscriminate access or misuse of the intercepted information.

Additionally, the Court stressed the importance of taking precautions when communicating the intercepted material with other parties entailing safeguarding sensitive information and preventing unauthorized access or disclosure, particularly when sharing data with foreign intelligence agencies or other government entities.

Moreover, the Court carefully examined the limits on the duration of interception activities and the storage of intercepted material. This implies that interception

[93] Tiberi G., *Il caso Big Brother Watch quale cambio di paradigma nel bilanciamento tra sicurezza e tutela dei diritti fondamentali?* in *Quaderni costituzionali*, *Fascicolo 4*, il Mulino, 2018, Bologna.

measures should not be conducted indefinitely, and that intercepted data should only be retained for as long as necessary for the legitimate purposes for which it was collected.

In terms of oversight, the Court emphasized the need for effective supervision by an independent authority to ensure compliance with the established safeguards. This means that an impartial oversight body should have the power to monitor and review interception activities, ensuring that they adhere to the principles of legality, necessity, and proportionality.

Lastly, the Court emphasized the significance of procedures for independent *ex post facto* review of compliance with interception safeguards. This entails a thorough assessment of the legality and proportionality of interception measures after their implementation. Additionally, competent bodies should be empowered to address instances of non-compliance promptly and effectively to ensure accountability and prevent further violations[94].

Once having established the new eight criteria, it was now time for the Court to assess to the concrete case at hand with a renewed legal background to support the future decision. In its evaluation of the United Kingdom's bulk interception regime, the Grand Chamber applied the newly established criteria and identified several significant "fundamental deficiencies". A primary concern revolved around the lack of independent authorization for the programs, as they were primarily based on authorization from the executive, specifically the Secretary of State. This lack of independent oversight raised red flags as it compromised the checks and balances necessary to ensure the legality and proportionality of surveillance activities.

Furthermore, the Grand Chamber highlighted issues regarding the specificity of categories of general selectors, or search terms, to be used in the interception programs. The absence of clear specifications in the law allowed for potential ambiguity and misuse, undermining the protection of individuals' right to privacy. A noteworthy aspect that drew the Grand Chamber's attention was the insufficient internal scrutiny of specific identifiers applied to individuals. This aspect further undermined the safeguards in place and raised concerns about the potential for unwarranted intrusion into individuals' private communications.

[94] Case of *Big Brother Watch and Others v. The United Kingdom*, cit., para. 361.

Similarly, the United Kingdom's program for bulk acquisition of metadata from service providers also exhibited similar deficiencies, drawing similar criticisms from the Grand Chamber. The lack of adequate restrictions on authorities' access to data and the absence of independent review mechanisms raised concerns about the legality and proportionality of this data collection practice.

The Grand Chamber's evaluation led to the conclusion that these programs were not "*in accordance with the law*" as they failed to meet the essential criteria set out by the Court. The lack of proper authorization, specificity, and internal scrutiny rendered these surveillance activities open to potential abuse and infringed upon the rights guaranteed by Article 8 of the European Convention on Human Rights. Additionally, the Court found that both bulk interception programs violated Article 10, which safeguards freedom of expression, particularly when it comes to journalistic sources and confidential communications. The programs lacked the necessary safeguards to protect the confidentiality of journalistic sources, potentially leading to a chilling effect on press freedom and undermining the ability of journalists to fulfill their critical role in society[95].

To conclude the examination of *Big Brother Watch*, some crucial issues which are linked to the outcomes of the decision will be closely analyzed in the next two paragraphs: firstly, the concurring and dissenting opinions annexed to the text of the decision will be closely examined as at least five of the judges composing the Grand Chamber delivered different point of views about the possible negative repercussions of the decision taken by the Court. Following, the issue of extraterritorial application of the European Convention on Human Rights will be approached as it seems that the judges of the Grand Chamber avoided to deal with this complex matter.

3.3 A Non-unanimous Decision: Dissenting and Concurring Opinions

According to Marco Milanovic, the ruling signifies a lasting establishment of mass surveillance as a standard practice for many years ahead[96]. Five of the justices who ruled the *Big Brother Watch* case were of this same opinion: indeed, at the end of the

[95] Lubin A., *Introductory Note to Big Brother Watch v. UK (Eur. Ct. H.R. Grand Chamber)* in *International Legal Materials*, 2022, 61(4).
[96] Milanovic M., *ECtHR Judgment in Big Brother Watch v. UK* in Ejitalk.org, 2018.

long decisioning text, concurring and dissenting opinions of several justices can be witnessed.

3.3.1 *Joint Partly Concurring Opinion of Judges Lemmens, Vehabović, Bošnjak, and Ranzoni*

The first one which can be identified is the joint partly concurring opinion delivered by judges Lemmens, Vehabovič, Bošnjak, and Ranzoni. The four judges found themselves aligned with the majority of the decision taken by the Grand Chamber with the exception of two operative points: from their viewpoint the judgment missed a valuable opportunity to fully support the importance of privacy and correspondence in the face of intrusions such as mass surveillance by not identifying any breach of both Articles 8 and 10 of the Convention concerning the receipt of intelligence from foreign intelligence services. According to the judges' opinion, there are rare instances when a Court ruling significantly shapes the future of our societies, and the Big Brother decision was one such example. The Grand Chamber had, to some extent, taken advantage of this opportunity and laid out a comprehensive set of principles aimed at safeguarding human rights and fundamental freedoms, particularly those protected under Articles 8 and 10 of the Convention. However, while conducting the balancing exercise, the majority had not adequately emphasized the importance of private life and correspondence, which, in several aspects, remained insufficiently safeguarded in the face of interference from bulk interception[97]. It seems reasonable to go deeper into the reasoning of the four judges.

Before explaining the key concepts behind their opinion, the four judges stated what privacy means to them by describing it as a "a fundamental precondition for a variety of fundamental individual interests, but also for the existence of a democratic society". Their description focused on the fact that the right to privacy "is essential for a person's well-being, autonomy, self-development, and ability to enter into meaningful relationships with other persons. It is also a necessary precondition for the enjoyment of civil rights and consequently for a person's status as a free and equal member of a

[97] Case of *Big Brother Watch and Others v. The United Kingdom*, Joint Partly Concurring Opinion of Judges Lemmens, Vehabović, Bošnjak, and Ranzoni, Judgment of the European Court of Human Rights, 2021.

democratic society". Any violation of this right could result in both diminishing individual autonomy and disrupting the democracy itself[98].

According to the four judges of the Grand Chamber, as the Court has managed to weigh private life and privacy of correspondence compared to the legitimate interests of a given state, it should have given a more significant importance to those two principles enshrined in Articles 8 and 10 of the Convention even from the point of view of the citizens. Three are the key points listed in the concurring opinion: a proper weight to interferences in the private life of the citizens and in the privacy of the correspondence should have been given, clearer safeguards against possible misuses of the bulk interception techniques should have been settled, and subsequently, a stricter evaluation of those bulk methods of collecting information should have been followed[99].

For the last of the three aforementioned points, the dissatisfied judges delivered a new point of view of the bulk interceptions phases previously recognized by the court. It was indeed established by the Grand Chamber that the bulk collection of private data is pursued by four stages: an initial interception stage, one in which specific selectors are applied, an examination phase of the selected data, and a final retention stage and subsequent use of the collected material considered useful for investigation purposes[100]. In describing each stage, the majority of the Grand Chamber stated that the initial stage "does not constitute a particularly significant interference". Judges contrary to this statement explained their disagreeing position. It is clear in the first instance that it is in the initial stage that individuals private information come into the hands of governmental authorities charged to investigate: in the judges mind it was essential to note that even if, in the initial stage, the content of these communications has not been examined or presented to decision-makers, meaning that no immediate action can be taken against any specific individual, this very first phase of investigation must be considered as an indispensable prerequisite for any of the three subsequent stages of analysis of the data.

[98] Ivi, para. 3.
[99] Ivi, para. 10.
[100] Case of *Big Brother Watch and Others v. The United Kingdom*, Judgment of the European Court of Human Rights, 2021, para 325.

Pursuing with the judges reasoning, it was true that the full scope of communications and related data gathered by intelligence services remained uncertain, but it was also crystal-clear that there were indications that a significant portion of millions of individuals' communications was regularly intercepted. The situation is further exacerbated by the fact that those affected are typically unaware of this intrusion. In such circumstances, where people cannot determine if their communications are intercepted but are conscious of a strong likelihood of it happening, there is a strong possibility that a radical change of behavior of their habitudes occurs, potentially leading to dangerous outcomes concerning a state's security.

To conclude their statement related to the stages of interception, the judges felt concerned about the discarding of not useful information within the one gathered: the majority of the Grand Chamber felt satisfied by the fact that "parts of intercepted communications are discarded immediately", but, in the opinion of the opposing judges, there were not enough clarifications on how the discarding of futile data was managed: "The very fact that this act is performed in obscurity and on an unknown basis should, in our opinion, be a matter of serious concern. Such a lack of transparency, at the very least, can hardly meet the requirement of foreseeability, this in turn being one of the preconditions for the lawfulness of any interference with the rights protected by Article 8 of the Convention"[101].

A fundamental contribution given by the judges concerned the eight new safeguards settled by the Grand Chamber: according to them, even if those safeguards could be useful tools against an arbitrary usage of interception methods, several issues have arisen and have been left untouched by the Grand Chamber. Firstly, these criteria did not seem to function as independent and absolute minimum standards. Secondly, while these criteria called for explicit definitions of specific safeguards within domestic law, they did not establish any minimum safeguard requirements themselves. Lastly, the criteria lacked explicit substantive protection for individuals against excessive interference, particularly concerning the application of strong selectors to collected material. Additionally, the procedural protection offered by these criteria was deemed insufficient[102].

[101] Case of *Big Brother Watch and Others v. The United Kingdom*, Joint Partly Concurring Opinion, cit., para. 11-12.
[102] Ivi, para. 14.

The wording of the first two new established safeguards was harshly criticized too, as even if the Grand Chamber had demanded to domestic legislations to specify the "*grounds"* on which bulk interceptions may be authorized together with the *circumstances* in which a citizen's private data may be intercepted, there was no clear indication of what these *grounds* and *circumstances* entailed or excluded[103].

Finally, in the very last paragraphs of the annexed joint partly concurring opinion, the judges made direct reference to the case at hand as, according to them, certain aspects of the decision concerning the UK's interception techniques had failed to adequately to pinpoint some drawbacks. A lack of clarity and transparency in the crucial area of what really were the interests of national security of the United Kingdom had been noticed. Within the British borders, as clarified by the majority of the Grand Chamber, a bulk collection of private data could be demanded "*in the interests of national security*, for the purpose of preventing or detecting serious crimes, or for the purpose of safeguarding the economic well-being of Great Britain insofar as those interests were also relevant to *the interests of national security*": in the concurring opinion it was underlined that in two out of the three purposes, the wording "*in the interests of national security*" was used, but no explicit definition of what an interest of national security could be was exemplified, possibly leading to a misuse of the interception methods.

3.3.2 *Partly Concurring and Partly Dissenting Opinion of Judge Pinto De Albuquerque*

Judge Pinto De Albuquerque complex contribution is probably the most complete within the concurring and dissenting opinion annexed at the end of the decisional text of the European Court of Human Rights. As it is deeply examined in the first part of the attached opinion of the dissenting judge, the Grand Chamber has developed a *pro-autoritate* decision: in the first part of the document, he proceeded deconstructing the final judgment of the Court considered to be excessively in favor of intelligence agencies' needs. Following, the judge delivered a new *pro-persona* point of view of the case: according to his opinion, the majority should have followed this path from the very beginning of the lawsuit. Lastly, based on what he established in the second part

[103] Ivi, para. 21.

of his dissenting point of view, he reformulated more suitable conclusions concerning the UK bulk interception regimes.

The deconstruction phase of his dissenting opinion is pursued by following three key steps: judge De Albuquerque harshly criticized the language used by his collogues, considered to be too vague and unclear, the methodology used to deal with the case, biased by several Court's inattentions and inaccuracies, and the new established safeguards, not enough clear in the obligations placed.

Making reference to the judge criticisms to the inadmissibly vague language used by the Court, according to him, the Grand Chamber's reliance on such an imprecise wording posed several noteworthy implications. Firstly, it left room for ambiguity and varied interpretations, which might lead to inconsistent application of the judgment across different cases and jurisdictions, potentially weakening the impact of the Court's decisions as a cohesive legal framework for safeguarding human rights. Secondly, when judges exhibit hesitation or uncertainty in their rulings, this may create doubts among stakeholders about the Court's capacity to uphold its mandate of protecting fundamental rights. This hesitancy might cast doubts on the Court's authority and hinder its ability to command compliance from member states. Moreover, this imprecise language could potentially undermine the standard-setting potential of the judgment. By not clearly delineating the boundaries and requirements for compliance, the judgment lost its capacity to serve as a guiding precedent for future cases, and its potential to shape the development of human rights law is diminished. In order to deal with the issue, the judge then proceeded by listing the key words used by the Court joined by a precise analysis of their meaning in order to not let anything to the imagination of a hypothetical reader[104].

Judge Pinto de Albuquerque disapproval on the methodology used by the Court could be resumed as it follows: issuing a judgment on a limited basis of information furnished by the UK government which clearly did not provide all the data needed by the Court to give a complete overview of the issue, paved the way for what the judge

[104] Case of *Big Brother Watch and Others v. The United Kingdom*, Partly Concurring and Partly Dissenting Opinion of Judge Pinto De Albuquerque, Judgment of the European Court of Human Rights, para 2-3.

defined as an "educated guess", a biased decision built on a self-imposed limitation which inevitably brought the majority considering bulk interceptions as unavoidable.

Moreover, in the same context of misleading conclusions provoked by the wrong methodology used, the judge severely criticized the Court's decision to abandon the previous case law: in three cases, including the already inspected *Zakharov v. Russia* case, the Court had followed a different judicial reasoning and, according to judge de Albuquerque, it had without any good reason departed from it while ruling on *Big Brother* judgment. The three main justifications provided by the Court to depart from the previous jurisprudence, did not satisfy judge de Albuquerque.

Firstly, the Court had stated that unlike targeted surveillance, bulk interceptions were used most of all to monitor communications outside the state's territorial jurisdiction, making the previously established safeguards obsolete: the judge deconstructed the Court's idea based on the fact that they did not provide any concrete proof of their statement. Conversely, several Government's admissions about the exact contrary could be witnessed.

Secondly, according to the Grand Chamber, bulk collection of data should not be disciplined by the same criteria of targeted interceptions because one main characteristic of the former is foreign intelligence gathering where there may be not a specific target making the technique departing from the previously targeted surveillance-related safeguards: according to judge de Albuquerque "nothing precludes the possibility that foreign intelligence gathering itself may be pursued by means of bulk interception based on a requirement of reasonable suspicion of the involvement of the targeted person or group of persons involved in activities harmful to national security" making the Court's point unsuitable as a justification.

Lastly, the Court contended that, regarding interception using strong selectors, devices of targeted individuals are not directly monitored. Consequently, the Court argued that bulk interception methods did not necessitate the same level of safeguards as traditional targeted interception: according to the dissenting judge, this was the weakest point of the Court as it was crystal-clear in the judge opinion that "The automatic collection and processing by means of strong selectors permitting the acquisition of electronic communications to, from or about the target across the bearers chosen by the intelligence services is a potentially much more intrusive form of

interference with Article 8 rights than the mere monitoring of the targeted individuals' devices"[105]

For which it concerns the final point of judge Pinto de Albuquerque's digression in deconstructing the Grand Chamber's decision, his criticism towards the defective regime of safeguards established by the ECtHR, he followed the same reasoning of the previously analyzed concurring opinion: the *grounds* and *circumstances* described in the first two points of the eight end-to-end safeguards were not enough clear in their meaning. The mandatory purpose of the safeguards was questioned by the judge as the Court used an imperative language alternated to a dilution of the safeguards in a comprehensive evaluation of the regime's operation, weakening the new-established criteria and permitting a compromise between them[106].

In sum, according to judge De Albuquerque, the decision of the Grand Chamber of the ECtHR not only has undermined the authority of the Court itself, but it has also reduced the significance of the judgment as a benchmark for future cases, opening the door for the responding states to exercise their own discretion in carrying out the terms of the ruling[107].

Once having deconstructed the new case-law established by the Grand Chamber, judge de Albuquerque managed to deliver a new citizen-oriented jurisprudence. A new point of view of bulk interception methods, exchange of intercept data with foreign intelligence services, and bulk interception of related communications data was given with the production of a deeper and more complex list of safeguards in order to avoid any possible violation of the right to privacy enshrined in Article 8 of the Convention.

To begin, the judge underlined the utility of the reasonable suspicion principle discarded by the Court in his judgment as part of the former, targeted surveillance-related, case-law established in the *Zahkarov v. Russia* ruling, to ensure the legitimacy of bulk interception: it is imperative that any target of bulk surveillance is always identified or identifiable in advance based on that principle. This requires employing strong selectors, specifically targeting communications from and to the intercept

[105] Ivi, para. 8-12.
[106] Zalnieriute M., *Big Brother Watch and Others v. the United Kingdom*, in *American Journal of International Law*, 2022, 116(3).
[107] Zalnieriute M., Big Brother Watch v. UK, in VerfBlog, 2 June 2021.

subject when there is a reasonable suspicion of their involvement in severe crimes or actions that could endanger national security.

Following, the process of judicial warranting was reviewed by the judge too: it should encompass the authorization of surveillance for communications and related data, including privileged and confidential information, except in urgent cases when immediate access to a judge is not feasible. In such urgent instances, public prosecutors may grant authorization, subject to subsequent endorsement by a competent judge. This full judicial empowerment should be accompanied by regular and vigilant oversight by the judge, scrutinizing the necessity and proportionality of the interception order in light of the data obtained throughout all the stages of interception. To this concern, the judge added the importance of an *ex-post* review at the end of the process of interception: in this final stage of reviewing the bulk surveillance order the action of notifying the targeted individual should be considered, enabling him to challenge the grounds for interception in a fair judicial procedure. In cases where notification of the person whose communications have been intercepted is not feasible due to national security concerns, it becomes crucial to burden the competent judge with assessing the lawfulness of the interception order's execution, determining whether the collected data should be retained or destroyed.

Throughout the establishment of safeguards, the judge introduced a new principle to be protected by the domestic law, which aimed to establish a specific protective regime for privileged professional communications of parliamentarians, medical doctors, lawyers, and journalists. Indiscriminate and suspicionless bulk collection of communications originating or received by those protected professions would undermine the protection of legally safeguarded and confidential information. Therefore, when there is proof establishing a reasonable suspicion that these experts are engaged in major felonies or actions detrimental to national security, a Court authorization should be necessary before such conversations could be intercepted. If those communications are inadvertently intercepted, they should be immediately deleted. Additionally, domestic legislation must categorically forbid the spying on communications governed by religious secrecy.

In considering the exchange of intercepted private data with foreign intelligence services or in more general terms, to third parties, the dissenting judge harshly criticized

that the majority did not ponder about the receiving states safeguards: since too low standards were set by the Court, judge de Albuquerque again emphasized the essential presence of a judicial oversight being as stringent as in any other scenario previously descripted.

Finally, the "*states' wide margin of appreciation deciding what type of interception regime is necessary*" wording was denounced as it was deemed to be not enough clear in specifying to what extent states could decide when to strengthen the control over its citizens: "If the boundaries of State discretion are wide, even the most stringent policing of them does little to safeguard against abuse"[108].

To conclude his fundamental contribution, the judge believed that a new analysis of the case at hand based on his previously examined fundings was needed starting from an analysis of bulk interception of communications under the RIP Act, then examining the UK's exchange of intercept data with third parties and concluding with providing a new point of view concerning the bulk interception of related communications data.

In applying the new safeguards to Great Britain's RIP Act of 2000, giving a personal judgment to UK's bulk interception regimes, one of the judge's major concerns was the insufficiently defined notion of "*national security*", leaving room for ambiguity and potential abuse of surveillance powers. Furthermore, the criteria for identifying individuals subject to interception were not well-specified within the UK legislation, particularly concerning the distinction between internal and external communications. The authorization process for section 8 warrants lacked independence, a fundamental principle previously emphasized by the judge, granting the Secretary of State a too broad discretion without proper checks and balances: this allowed for interceptions without clear identification of the targets, limitations on the number of intercepted communications, or specific guidelines on bearers and selectors used for interception. Moreover, the absence of a binding code of practice issued by the Secretary of State, along with the possibility of departing from it for not well specified reasons, raised concerns about accountability and adherence to proper procedures. The same lack of independence was witnessed by the judge in the figure of the IC Commissioner, which did not provide an effective oversight of the implementation of the interception warrant: according to the judge, in terms of oversight, the presence of an independent body was

[108] Ivi, para. 16-34.

essential to ensure the legitimacy and legality of surveillance activities, and the absence of such a body within the IC Commissioner's framework pointed to a significant flaw in the system. Another notable gap was the absence of specific rules for professionals, contrasting with the proposed new safeguards suggested by Albuquerque. The legislation's vagueness finally extended to the duration of interception and subsequent notification protocols, leaving room for arbitrary decisions and inadequate protection of individual rights.[109]

The majority's stance on the transfer of bulk material to foreign intelligence partners was also subject to judge de Albuquerque's scrutiny. While the Court acknowledged the need for an independent control for such transfers, it appeared to diverge when it came to the receipt of bulk material collected by foreign intelligence authorities. This discrepancy raised questions about the consistency and adequacy of safeguards when data is received from foreign partners. An example made by the judge in paragraph 52 could help unravelling the conundrum: assuming that one Londoner had sent a message to another via a server in the United States, the interception of this communication by the GCHQ when it left the United Kingdom warranted the guarantee of independent authorization, according to the Court. However, if the same message was intercepted by the NSA at the other end of the same cable and then shared with GCHQ, or the communications data relating to it, the guarantee of independent authorization no longer applied[110].

Finally, bulk interception of related communications data, that is to say all secondary data that are contained in a digital message such as Ip addresses or communication equipment used, was also reviewed in the final paragraphs of judge de Albuquerque's dissenting opinion. Since any direct reference to "*related communication data*" was not set out in the legislation, the RIP Act simply could not be applied to this kind of private information, paving the way for any analyst to circumvent the Act, allowing them to obtain private details of individuals by not formally violating any law[111].

The final words of judge Pinto de Albuquerque are crystal-clear to summarize his opinion on the judgment of the Grand Chamber's majority: "In the present judgment the Court has succumbed to the *fait accompli* of general bulk interception, dangerously

[109] Ivi, para. 36-49.
[110] Ivi, para. 52.
[111] Ivi, para. 55.

accepting that if it is useful, it should be permissible. Usefulness is not the same thing as necessity and proportionality in a democratic society"[112].

3.4 The Question of Extraterritoriality: is the European Convention of Human Rights Universal?

Extraterritoriality is a principle in international law that allows certain laws or legal obligations to be applied outside the boundaries of a state's territory. This principle enables states to exercise jurisdiction over certain actions or individuals that have a connection with their territory, even if the actual conduct occurs outside of it. The rationale behind extraterritoriality is to ensure that states can protect their interests, maintain security, and uphold their values beyond their borders[113]. As underlined by professor Milanovic in his commentary over the *Big Brother Watch and Others v. the United Kingdom* case, this quite complex issue which was not dealt by the Court and it is worth to be descripted in this paragraph: the extraterritorial application of the European Convention of Human Rights outside the borders of the Council of Europe, has been put aside by the judges of the Court as it poses enormous decisional complexities. The reason why the Court has had the possibility to ignore the principle while ruling the final judgment could be identified in the United Kingdom's missed opportunity to raise objections related to a possible application of the Convention on non-European citizens: this assisted the Court in simply assuming the obviousness of the external applicability of the Convention, permitting the First Section Chamber in first instance, and subsequently the Grand Chamber, to directly deal with the merits of the case[114].

The situation is obviously much more complex as Article 1 of the ECHR comes in the foreground. As it is stated in the first article of the text "*The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of the Convention*"[115]. Article 1 of the Convention places certain responsibilities of effective governance on each Contracting Party concerning

[112] Ivi, para. 58.
[113] Lawson R., *Life After Bankovic: On the Extraterritorial Application of the European Convention on Human Rights* in Coomans F. and Kamminga M. (eds), *Extraterritorial Application of Human Rights,* Intersentia, 2004, 83-123.
[114] Milanovic M., *ECtHR Judgment in Big Brother Watch v. UK*, cit.
[115] European Convention on Human Rights, Article 1.

individuals under its authority. These obligations, however, are specifically limited to those individuals who are within the territory of the contracting party. As a result, for someone to claim that their rights under the Convention have been violated, it must be shown that they were indeed within the territory of the state in question at the time when the alleged violation occurred. The meaning of the wording "*within their jurisdiction*" sounds vague and has remained a controversial point to be discussed within the legislative framework of the Council of Europe since its earliest days. When determining the obligations of Contracting States for alleged human rights violations allegedly taking place outside of their territories during extraterritorial activities, contracting states of the ECHR frequently support a more constrained interpretation of the wording "*within their jurisdiction*" under Article 1. In these situations, the respondent governments frequently contend that the notion of jurisdiction under Article 1 is primarily tied to geographical limits and that any expansion outside of the State's territory should be regarded as unusual or extraordinary. In this regard, over the last two decades, the Court has faced harsh criticism for struggling to create a unified, consistent, and clear legal framework although it has issued numerous rulings regarding the extraterritorial actions of the contracting states.[116].

A landmark decision worth to be mentioned is the 2001 judgement of *Banković and Others v. Belgium and 16 Other Contracting States*. The decision departed from the early case law of the XX century which was based on the firm idea that the responsibility of a State is not confined solely to its territory but encompasses all individuals under its actual authority and responsibility regardless of whether this authority is exercised within its own borders or abroad. Indeed, decisions made in the *Banković* case reflected a stricter way of understanding the meaning of Article 1 of the Convention: the provision should be understood in its ordinary and primarily territorial sense, with other bases of jurisdiction considered exceptional and requiring specific justification in each case. In particular, the Court deemed the activities of a state's air forces in another country to be outside the scope of the Convention's jurisdiction, and the circumstances of the case did not warrant an exceptional situation where the victims could be considered under the jurisdiction of the respondent governments: indeed, it

[116] Karakaş I. and Bakırcı H., *Extraterritorial Application of the European Convention on Human Rights: Evolution of the Court's Jurisprudence on the Notions of Extraterritorial Jurisdiction and State Responsibility*, in A. van Aaken, I. Motoc (eds.), *The European Convention on Human Rights and General International Law*, Oxford, 2018, ch. VI.

emphasized that the Convention's protection was limited to the legal space of the contracting states, further narrowing the *effective control* exception by distinguishing between territories within and outside the Convention's legal scope. Moreover, it was suggested that the Convention might not impose an obligation to protect the rights of residents in occupied territories if they had not previously been entitled to such rights under the Convention[117].

Although it pronounced against the application of the Convention outside the territorial limit of the contracting states of the ECHR, the Court managed to develop four exceptions based on the previous jurisprudence in which the extraterritorial application of the European legislation could be possible. These exceptions encompass specific situations where the ECHR's protection extends to individuals even outside a member state's territory. One such exception arises in cases of extradition or expulsion: when a member state decides to extradite or expel an individual from its territory, issues regarding potential mistreatment or even death of the individual or group of people in the receiving country may arise, thereby invoking the applicability of Article 2 or 3 of the ECHR. In extreme circumstances, issues related to detention or trial conditions may also fall under the scope of Article 5 or 6. Moreover, the Court has recognized extraterritorial effects cases, where state actions occurring outside their own territory could lead to significant consequences: these cases involve actions or decisions by state authorities that have far-reaching effects beyond their borders, allowing the ECHR to be applied to such situations. Additionally, the principle of effective control plays a crucial role in extending the ECHR's jurisdiction. If a member state, through military action, whether lawful or unlawful, gains effective control over an area outside its national territory, the Court may consider the ECHR applicable in those circumstances. Lastly, consular or diplomatic cases, as well as flag jurisdiction cases, are also subject to the ECHR's reach. These cases involve the activities of a member state's diplomatic or consular agents abroad[118].

The jurisprudence around the extraterritoriality principle has been furtherly developed by the Court in subsequent judgments: here below the major decisions

[117] Ibidem.
[118] Miller S., *Revisiting Extraterritorial Jurisdiction: A Territorial Justification for Extraterritorial Jurisdiction under the European Convention* in *The European Journal of International Law*, 2009, 20(4), 1223–26.

concerning the extraterritoriality principle will be briefly examined in order to give a deep comprehensive knowledge of the concept of extraterritoriality.

Six shepherds were killed in northern Iraq in April 1995 as a result of Turkish army military activities, according to the lawsuit of *Issa and Others v. Turkey*. The Court lacked confidence in the Turkish army's ability to effectively manage the region where the killings took place or in the shepherds' prior subordination to Turkish soldiers. In light of this, the Court came to the conclusion that Turkey did not have jurisdiction over the deceased people in accordance with Article 1 of the Convention. However, the Court argued that the shepherds would logically be under Turkish jurisdiction rather than Iraq's, which is not a Contracting State and is outside the legal space of the Contracting States, if it had been established that the Turkish army forces were, even briefly, in effective control of the area in question[119].

The application of the Convention outside the boundaries of a contracting state under the *effective control* principle was extended to ad hoc police operations on a foreign territory too in the *Öcalan v. Turkey* judgment of 2005: the Court decision contributed to the expansion of the extraterritorial application of the Convention exceptions jeopardizing its jurisprudence. Considering its extraterritorial component, the question of whether the Convention might be applied to the matter of the applicant's arrest in Nairobi, which occurred outside the Turkish territory, an ECHR's contracting state, indeed outside the ECHR's "legal space", has arisen. The usual norm that the idea of jurisdiction under Article 1 is territorial is defied by the *Öcalan* judgment: the evident justification for the exemption is that Turkey was effectively controlling the applicant inside Kenya's territory while operating the police operation with the African's state approval[120].

Departing from the *Bankovic* findings, the Court has reviewed the extraterritorial applicability of the Convention in the 2011 *Al-Skeini and Others v the United Kingdom*. The judgment marked a significant turning point within the legal framework of the principle as not only the Court declared that contracting states must uphold their human rights obligations wherever their agents exercise authority and control over individuals, but it also confirmed that the Convention's application goes beyond the boundaries of

[119] Ibidem.
[120] Gondek M., *Extraterritorial Application of The European Convention on Human Rights: Territorial Focus in the Age of Globalization?*, in *NILR*, 2005, 52(3).

Council of Europe's countries and expanded the concept of the "European legal space" that was proposed in the Banković case. In particular, the United Kingdom assumed responsibility for exercising several public functions that are ordinarily within the authority of a sovereign government in Iraq. It specifically took over control and accountability for preserving security in the nation's southeast. The British forces actively engaged in security operations in Basra in this particular instance exerted the country's jurisdiction over the killing of six Iraqi nationals: given that, according to the Court, the United Kingdom had the responsibility to at least guarantee to the victims the right to life enshrined in Article 2 of the Convention since its authority was manifested through its soldiers[121].

The last case at stake is the *Jaloud v. The Netherlands* decision of 2014 in which, working towards a further expansion of the exceptions established in the *Banković* decision, the Court established that outside the Council of Europe boundaries, in Iraq in this specific situation, even in the lack of an actual authority over the land in query, the mere practice of exercising authority over a checkpoint is sufficient to establish the jurisdiction of a contracting state. While the Dutch government tried to prove that the killing of the son of the applicant had to be attributed to the United States and the United Kingdom as "occupying forces" under the United Nations Security Council Resolution 1483 and that the Low Countries had never assumed the public powers typically imputed to a sovereign government, the Court stated that a given country could not circumvent the obligations laid down in the Convention just because it fulfilled another state request: the applicant's son had been fatally shot at a checkpoint supervised by individuals under the direction and direct control of a Dutch army officer, and that was sufficient, in the Court's opinion, to shift the responsibility to Netherlands[122].

It has recently become clear that people are particularly vulnerable when faced with State acts that are increasingly crossing international borders. The Court has had to address numerous cases over the past twenty years as a result of the Contracting States' extensive extraterritorial activities. These cases have raised issues regarding whether or not states can be held accountable for violations of the Convention outside of their own borders. In this regard, thanks to the work of the ECtHR within the last two decades,

[121] Karakaş I. and Bakırcı H., *Extraterritorial Application of the European Convention on Human Rights: Evolution of the Court's Jurisprudence on the Notions of Extraterritorial Jurisdiction and State Responsibility*, cit.
[122] Ibidem.

the wording "*within their jurisdiction*" in Article 1 of the Convention does not only refer to a territorial concept of jurisdiction anymore, but it has been expanded with a more complex and deeper legal basis[123]. However, it has to be stated that the principle of extraterritoriality, as anticipated in very first lines of this paragraph, has never been dealt by the Court in the context of intelligent services operations collecting vast amount of data of foreign citizens as it could pose enormous complexities in reaching unanimous decisions: throughout the entire *Big Brother* judgmental text, there is no single reference to the principle of extraterritoriality with the mere exception of judge Pinto de Albuquerque's dissenting opinion. Indeed, in paragraph 33 of his contribution, in enumerating his personal enhanced safeguards concerning his *pro-persona* judgment of *Big Brother,* he specified that "These principles apply to surveillance conducted in the Contracting Party's own territory as well as to its surveillance performed *extraterritorially*, regardless of the purpose for the surveillance, the state of the data (stored or in transit), or the possession of the data […]"[124]. The main critical issue that emerges from the dissenting judge's words is that still not enough reference to the extraterritorial application of Article 8 of the European Convention of Human Rights has been made. A similar deficiency has been witnessed in the *Centrum För Rättvisa* judgment, an ECtHR ruling parallel to the *Big Brother* case which will be briefly examined in the following paragraph.

3.5 A Parallel Decision: Centrum För Rättvisa v. Sweden

Centrum För Rättvisa v. Sweden is a 2021 judgment on which the Grand Chamber of the European Court of Human Rights was called to deliberate parallelly to the *Big Brother Watch* decision: in this regard, the two rulings should not be read independently in order to reach a major comprehensive knowledge of the right to privacy legal framework recently developed by the ECtHR. Throughout this paragraph the case will be briefly analyzed trying to understand if the Court had reached different findings from the ones of the *Big Brother Watch* decision, or if, on the other hand, it had followed the same reasoning.

[123] Ibidem.
[124] Case of *Big Brother Watch and Others v. The United Kingdom*, Partly Concurring and Partly Dissenting Opinion of Judge Pinto De Albuquerque, cit., para. 33.

The lawsuit was filed by the non-governmental Swedish organization Centrum För Rättvisa, which main aim is to promote the protection of fundamental human rights. The organization challenged the Swedish domestic legislation which allowed secret surveillance regimes based on signals intelligence, where the wording "*signals intelligence*" should be intended as "obtaining, collecting, processing and reporting information from electronic communication channels", considered to be in violation of Article 8 of the European Convention of Human Rights[125]. The applicant's criticism concerned the powers in the hand of a branch of the Swedish Ministry of Defense charged of signals intelligence, the National Defense Radio Establishment, granted by three provisions in particular: the two 2000 Act on Foreign Intelligence and Regulation of the Minister of Defense on Signals Intelligence and the 2008 Act on Signals Intelligence. In particular, the Act on Foreign Intelligence governs the extent to which intelligence operations can be conducted within the country's borders. These operations are limited to activities that are connected to matters outside the nation's boundaries. The specific objectives and guidelines for foreign intelligence activities are determined by the government. It is important to note that actions performed under this Act must not involve criminal investigations or activities reserved for the police services, which are responsible for crime detection and prevention. On the other hand The Act on Signals Intelligence, of which the scope of its application is well outlined in its first Article, provides a comprehensive list of criteria that warrant the utilization of electronic surveillance methods[126].

The main difference between the two decisions of the ECtHR can be witnessed in the Chamber of First Section deliberation. Indeed, if in the *Big Brother Watch* judgment a violation of Article 8 of the Convention has been identified since the very first paragraphs of the decisional text, and the Grand Chamber agreed with the Chamber of First Section's resolution in almost each aspect of the prior ruling, the situation in *Centrum För Rättvisa* was quite different: the Chamber did found the Swedish legislation regulating mass surveillance practices in accordance with the Convention, indeed not witnessing any violation of the right to privacy enshrined within the

[125] Vogiatzoglou P., *Centrum for rattvisa v sweden: Bulk interception of communications by intelligence services in sweden does not violate the right to privacy*, in *Eur. Data Prot. L. Rev.*, 563, 2018, 4(4).
[126] Rojszczak M., *The ECtHR's Judgment in the Case of Centrum För Rättvisa v. Sweden as a Leading Case for the Review of Domestic Regulations on Signals Surveillance* in *Review of International, European and Comparative Law*, 2019, 17, 84-103.

European source of law. In particular, throughout the analysis of the Chamber which mainly verted on the Act of Signals Surveillance, the Court recognized that a sufficiently comprehensive list of justifications to conduct such surveillance has been established by the Swedish legislation. Moreover, several documents presented during the legislative process permitted an expansion of such list, making the provision comply with the European Court of Human Rights case law. As the Court noticed in 2018, other aspects of the Swedish provision complied with the previously settled safeguards too: several independent oversight authorities were identified in bodies like the Court for Foreign Intelligence, the Ombudsman, the Personal Data Protection Office, and the parliamentary Committee for Defense, with the former in particular charged to check the proportionality and the necessity of the employed mass surveillance techniques. A maximum time duration of six months for the tapping activity was settled by the Act as well as criteria related to a possible extension of the operations and to the storage or further use of the collected data. Finally, the First Section's Court underlined that not only the Swedish domestic law adequately regulated the transferring activity of the data collected to third parties, with particular reference to foreign intelligent partners, but it also contained an abundant number of safeguards guaranteeing appropriate legal remedies to individuals who have been placed under monitoring[127]. As it has been already anticipated, in its final judgment, the Chamber "found that the Swedish system of signals intelligence provided adequate and sufficient guarantees against arbitrariness and the risk of abuse. The relevant legislation met the "*quality of law*" requirement, and the interference could be considered as being "*necessary in a democratic society*". Furthermore, the structure and operation of the system were proportionate to the aim sought to be achieved"[128].

The work of the Grand Chamber ended in overturning the First Section's Chamber decision. In order to reach the final result, the Court has followed an almost identical reasoning to the *Big Brother*'s one: in most of the paragraphs even the same wording can be witnessed. In this regard, several are the points of the Court reasoning which have already been dealt in the paragraph dedicated to the *Big Brother* judgment: in analyzing the bulk interception process, different degrees of interference were

[127] Ibidem.
[128] Case of *Centrum För Rättvisa v. Sweden*, Judgment of the European Court of Human Rights, 2021, para 181.

identified within four stages of the bulk interception activity; the same, harshly criticized by judge Pinto de Albuquerque, recognition of bulk interception techniques mainly employed for foreign intelligence gathering was made; the six minimum safeguards, highlighted in the *Zakharov* decision, were reviewed and updated as the first two criteria were again considered not readily applicable to a bulk interception regime as opposed to targeted surveillance; the requirement of "*reasonable suspicion*", which was considered to be unsuitable to a mass surveillance program, was assessed[129].

The Court's findings permitted it to review the case at hand. Its work did not focus on the Swedish surveillance activities' bases in domestic law, nor on the legitimate aims in the interest of national security of the same provisions, or even on the public accessibility of the law: the Court considered the three aforementioned points already sufficiently clear. Instead, the Grand Chamber focused on trying to understand if the domestic law "contained adequate and effective safeguards and guarantees to meet the requirements of *foreseeability* and *necessity in a democratic society*"[130]. By placing the Swedish provisions under a strict analysis from the point of view of the new established eight criteria, the Grand Chamber mainly found itself in accordance with the prior judgment: the Swedish Act of Signals Intelligence relied on adequate legal standards, provided clear grounds for surveillance authorizations and circumstances under which communication could be intercepted, correctly regulated the duration of an interception and adequately monitored the procedures to be followed in collecting and analyzing the intercepted data. Moreover, a well working judicial oversight body, identified in the Foreign Intelligence Court, was witnessed.

Indeed, three are the main deficiencies which pushed the Grand Chamber to overturn the prior judgment of the Chamber of First Section: firstly, the lack of a definite guideline for disposing of intercepted data devoid of personal information; secondly, the absence of a requirement to consider individuals' privacy concerns when sharing intelligence material to foreign intelligent agencies; finally, the shortage of an efficient retrospective review process. The existing safeguards did not adequately address these shortcomings, leading the Court to conclude that the Swedish bulk interception regime exceeded the margin of appreciation given to the authorities of the country in question: In its assessment, the Court stated that the Swedish bulk interception system lacked

[129] Ivi, para. 236-278.
[130] Ivi, para. 279.

adequate "end-to-end" safeguards to ensure effective protection against arbitrariness and the potential for misuse, consequently violating Article 8 of the Convention[131].

For which it concerns the final decision, some judges found themselves not completely in accordance with the majority and that led them to deliver concurring opinions. Worth to be mentioned is again judge Pinto de Albuquerque's intervention: in *Big Brother Watch* he had declared that his opinion should be read parallelly to the one's annexed at the end of the decisional text of *Centrum För Rättvisa* in order to fully understand his opinion in the context of balance between national security and privacy needs. Indeed, the statements furnished by the judge were based on the same reasonings behind his *Big Brother Watch* decision: the Court made the astonishing mistake of assuming the truthfulness of the Swedish government's assertations without having any concrete evidence about the veracity of what Sweden claimed to be their intelligent practices. Moreover, The Court was unable to obtain the pertinent case-law from the appropriate domestic court specializing in bulk interception, thus disregarding essential elements like the Foreign Intelligence Court's actual interpretation of section 3 of the Signals Intelligence Act. Based on those considerations, the judge was able to develop a conclusion similar to his one reached in *Big Brother Watch*: a biased methodology and a too vague language used by the Court brought to the establishment of a defective regime of safeguards[132].

Other scholars too dwelled on the subject trying to examine the Court's point of view. Indeed, Professor Asaf Lubin, associate Professor of Law at Indiana University Maurer School of Law has underlined in his analysis of the case that there is the possibility that in its efforts to legitimate the Swedish foreign surveillance machine, the ECtHR has tipped the scales too far in favor of more intrusive technologies. Accepting that the right to privacy needs to be changed to take into account the distinctive features of foreign spying should not mean that the Court's fundamental safeguards are abandoned or that we turn a blind eye to the bad effects of the practice: adjustments should be made with care and finesse, but according to the Professor, the Court seems

[131] Ivi, para. 367-374.
[132] Case of *Centrum För Rättvisa v. Sweden*, Concurring Opinion of Judge Pinto De Albuquerque, Judgment of the European Court of Human Rights, 2021, para 1.

to have operated "less like a surgeon in an operating room and more like an elephant in a China shop"[133].

3.6 A Victory for Privacy Rights or Priority to Security Needs?

In recent years, the rapid advancement of technology has transformed the way governments and corporations collect, store, and analyze personal data. This evolution has ignited debates over the delicate balance between safeguarding national security and protecting individuals' right to privacy. The case of *Big Brother Watch and Others v. United Kingdom* brought these concerns to the forefront of legal scrutiny.

The *Big Brother Watch and Others v. United Kingdom* and the *Centrum För Rättvisa v. Sweden* cases are often considered landmark rulings for privacy advocates because they highlighted significant concerns regarding mass surveillance and its potential impact on individual privacy. The ECtHR judgments emphasized the importance of striking a balance between national security interests and protecting individuals' right to privacy, as enshrined in Article 8 of the European Convention on Human Rights: here, the Strasbourg Court declared that there were indeed violations of Art. 8 of the Convention. However, despite being seen as a victory for privacy rights in some respects, the cases also represented an apex in achieving the opposite.

In earlier cases concerning the bulk interception of communications, such as the already deeply analyzed *Roman Zakharov v. Russia*, the European Court of Human Rights not only questioned the compatibility of such domestic surveillance measures with Convention rights, but also established a strict requirement for the presence of "*reasonable suspicion*" against a citizen before authorizing surveillance. However, in its 2018 judgements of *Centrum för Rättvisa v. Sweden* and *Big Brother Watch*, the Court took a different stance, endorsing the use of bulk interception of foreign communications. The Court asserted that this practice is a valuable tool to achieve legitimate objectives, especially considering the current threat level posed by global terrorism.

[133] Lubin A., *Legitimizing Foreign Mass Surveillance in the European Court of Human Rights* in *Just Security*, 2 August 2018.

The Court's decision to validate the UK's bulk interception regime, despite identifying certain deficiencies, has raised concerns among privacy advocates. The outcomes of the *Big Brother Watch* and *Centrum För Rättvisa* cases are considered unfavorable for privacy rights because they seem to prioritize national security interests over individual privacy. The validation of bulk interception practices, despite the identified deficiencies, raises concerns about the potential erosion of privacy rights in the digital age. Privacy activists argue that the Court's decision may set a precedent that could be used to legitimize intrusive surveillance practices without adequate safeguards, potentially setting back the protection of privacy rights for individuals within the UK and across Europe.

Four are the key aspects which may drive people considering *Big Brother Watch* and *Centrum För Rättvisa* cases in favor national security instead of privacy rights: bulk interception powers not being declared unlawful, necessity and proportionality principles analyzed from a new point of view closer to security needs than citizens' rights, a subsequent legislation, particularly in the United Kingdom, with newly expanded surveillance powers in the hands of the governments, and the obvious global impact of the case[134].

For which it concerns the first point of the four aforementioned key aspects, while the ECtHR acknowledged the privacy concerns raised by the applicants and recognized that the UK's surveillance practices required stricter safeguards and oversight, the Court did not declare the mere existence of bulk interception powers as unlawful. This meant that the rulings did not outright prohibit the use of mass surveillance techniques by the governments, leaving the door open for continued bulk data collection.

Regarding how the Court has dealt with the principles of necessity and proportionality, the ECtHR emphasized the importance of those principles when it comes to surveillance measures: it indicated that, under certain circumstances, bulk interception and data collection could be justified for national security purposes. This provided a legal avenue for governments to continue justifying extensive surveillance efforts if they can demonstrate that such measures are essential and proportionate to the threats they aim to counter.

[134] Watt E., *Much Ado About Mass Surveillance – the ECtHR Grand Chamber 'Opens the Gates of an Electronic "Big Brother" in Europe' in Big Brother Watch v UK*, Strasbourg Observers, 2021.

For which it concerns the subsequent legislation, following the *Big Brother Watch* decisions, the UK government enacted the Investigatory Powers Act 2016 (IPA), often referred to as the "Snooper's Charter". The IPA expanded the government's surveillance powers, broadened the scope of data collection, and granted authorities the ability to access citizens' internet browsing history without requiring a warrant. While the IPA included some improvements in terms of oversight, it also raised further concerns about the potential erosion of privacy rights: as stated by a wide number of scholars, the United Kingdom could currently claim that its mass surveillance system does not inherently contravene the European Convention on Human Rights, and that it will take the necessary measures to align itself with the stipulations set out by the European Court of Human Rights with relatively little difficulty[135]. Even Snowden has managed to comment the United Kingdom's new amplified surveillance system by defining it as "the most extreme surveillance in the history of western democracy"[136].

Finally, referring to the implications, as it can be easily expected, they go far beyond the UK and Sweden, as they have influenced discussions about surveillance practices and privacy rights in other countries as well. Some governments may have viewed the ECtHR's decision as a validation of the legitimacy of certain surveillance activities, potentially leading to increased surveillance measures in other jurisdictions: the Great Chamber decisions could possibly open the gates for a perpetual electronic "Big Brother" in Europe[137].

In describing the new safeguards set by the Court as, at the very least, "innovative", ICJ Senior Legal Advisor Massimo Frigo found himself dismayed by the Courts' final ruling: the Grand Chamber's decisions missed the chance given by these cases to confront the technological revolution of the previous decade, making only small improvements in safeguarding human rights in the digital era. Moreover, according to the legal expert's opinion, the inability of the Court to acknowledge and adequately control the moment of data collecting risks becoming fatal to the capability of the

[135] Sajfert J., *The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights,* in *EuLawBlog*, 8 June 2021.
[136] Pohle J. & Audenhove L. V., *Post-Snowden Internet Policy: Between Public Outrage, Resistance and Policy Change* in *Media and Communication*, 2017, 5(1), 1-6.
[137] Ibidem.

guarantees created by the Court to effectively safeguard the human rights of those who are exposed to this sort of monitoring[138].

3.7 Conclusions

In conclusion, the analysis of the *Big Brother Watch* case has been a central focus of this chapter, with its examination spanning several sections. After a brief introduction, the case was thoroughly introduced in the final chapter of the thesis, encompassing a comprehensive analysis of the applicants' claims and the successive decisions rendered by the prior Chamber of First Section and later by the Grand Chamber. The Grand Chamber ultimately found a violation of Article 8, which led to the establishment of vital privacy safeguards, marking a significant milestone in the realm of digital surveillance and data protection.

In delving deeper into the case, throughout the chapter, light has been shed on the diverse perspectives offered by the members of the Grand Chamber through their concurring and dissenting opinions. These viewpoints have provided a broader understanding of the complex dynamics at play, with particular attention paid to Judge Pinto De Albuquerque's partly dissenting and partly concurring opinion. His critique of the majority's decision, stemming from concerns over a biased methodology and vague language, offered valuable insights into the intricacies of the case. Overall, Judge Pinto De Albuquerque's opinion, together with the joint partly concurring opinion delivered by judges Lemmens, Vehabović, Bošnjak, and Ranzoni, offers an alternative perspective on the case, highlighting fundamental differences in how the case should have been approached and decided. These divergences provide a more comprehensive understanding of the complex issues at stake and the varying views within the Grand Chamber.

Furthermore, the matter of extraterritoriality has been addressed, as it emerged as a pertinent issue that the Court had avoided during the *Big Brother Watch* rulings to avert potential challenges throughout the decision-making process. This examination has provided additional depth to the analysis and illuminated the legal complexities

[138] Frigo M., *Big Brother Watch v. UK: A Landmark Judgment Missing the Mark*, International Commission of Jurists, 4 June 2021 [Online], Available at: https://www.icj.org/big-brother-watch-v-uk-a-landmark-judgment-missing-the-mark/.

involved in cases with cross-border implications: several cases in the hands of the ECtHR during the last two decades were brought to the foreground trying to furnish the most comprehensive approach possible to the principle of extraterritoriality. With these cases it was tried to underline the complexities and challenges associated with the extraterritorial application of surveillance and privacy laws, highlighting the need for careful consideration of cross-border implications and international legal principles: the balance between national security interests and the protection of privacy rights becomes particularly delicate when surveillance activities extend beyond a country's borders.

In a comparative analysis, the throughout the last paragraph of the chapter, the parallel judgment of *Centrum for Rattvisa* has been explored, identifying both similarities and differences with the *Big Brother Watch* case. This analysis of the cases was intended to further contribute to the understanding of how the Court addresses issues of privacy and data protection across the new technological era.

In conclusion, this last chapter has offered a comprehensive examination of the Big Brother Watch case, delving into its core aspects, the divergent opinions of the Grand Chamber members, the extraterritoriality question, and a comparative assessment with *Centrum För Rättvisa*. The insights gained from this analysis tried to provide a contribution to the broader discourse on the protection of privacy rights in the digital age. As technology continues to advance and new challenges arise, the legal community will undoubtedly draw from the lessons gleaned from landmark cases like *Big Brother Watch* and *Centrum För Rättvisa* to forge a more secure and privacy-conscious future.

CONCLUSIONS

This research has tried to analyze the evolutionary trend of the right to privacy within the Council of Europe and European Union boundaries throughout the last decades. The main interrogatives which drove the work are the following: has the European Court of Human Rights, in its latest judgments concerning mass surveillance and bulk interception techniques that are equally beneficial and intrusive, effectively managed to protect the right to privacy? Did the Court take the trade-off between individual liberties and public safety too lightly or was the right to privacy upheld to a full satisfaction?

As the examination begun, the first chapter of the thesis served as an introduction to the concept of the right to privacy. After a brief digression to explore the main features of the dichotomy between security and the right to privacy, which permitted the analysis of the concepts of proportionality, consent and accountability, the research has followed three distinct paths: national, European Union and Council of Europe legal frameworks concerning the aforementioned right were brought into the foreground, and a climax was reached with the examination of the ECtHR controversial landmark decision of *Zakharov v. Russia*, a 2013 judgment which saw the Council of Europe's main judicial body dealing for the first time with the new, intrusive and technological techniques of investigation employed by Russian intelligence services.

"Controversial", the word used to describe the sentence, is not casual, as while ruling on the case the Court has developed an particularly innovative approach towards mass surveillance: if on the one hand the Court stated that a system in which the secret services and the police have direct access, by technical means, to all mobile telephone communications presents a particularly high risk of abuse, openly violating art. 8 of the European Convention of Human Rights, on the other hand it decided to establish some precise criteria which, if respected, could guarantee to any government the possibility to conduct perpetual intrusive interceptions at the expense of the unsuspecting citizens. Those safeguards, known as the "six Weber Criteria" set an unprecedented standard to be followed in the rulings to come.

As the Snowden revelations have been examined throughout the second chapter, it has been recognized how the whistleblower managed to commence a domino effect which undermined the stability of the world security system by revealing the existence

of several mass surveillance programs indiscriminately conducted by both the North American National Security Agency and the British Government Communication Headquarters codenamed Tempora and Prism.

The disclosing has had an obvious effect at a legislative level too, paving the way for the landmark *Big Brother Watch* case closely analyzed throughout the third chapter of the thesis. The analysis of the judgment, conducted parallelly to the examination of the temporally simultaneous ruling of *Centrum För Rättvisa v. Sweden*, was the peak of the work trying to answer the questions which drove the entire thesis.

Following the same reasoning behind the *Zakharov* ruling, the European Court of Human Rights' Grand Chamber found a violation of article 8 of the ECHR, but again, the final deliberation of the Court could at least be considered questionable. Indeed, as many scholars opined, the Court has lost the opportunity to center a correct balance between security and privacy rights: in fact, while analyzing the case at stake, the Court only recognized the impossibility for the standards set out in the *Zakharov* ruling to be correctly applied to the *Big Brother* and *Centrum För Rättvisa* judgments because of the technological differences which characterized the techniques conducted by the Russian and British intelligent agencies in the two distinct situations. In light of this, the Court developed a security-driven judgment, by downgrading the previously set standards. In sum, the Court's Grand Chamber limited itself to a modification of the aforementioned "six Weber criteria", lowering them to the new technological means used by the GCHQ.

Namely, the Court emphasized the following: any law permitting more intrusive means to conduct investigations trying to find possible threats to democracy must clearly and explicitly state the grounds on which bulk interception may be authorized and the circumstances under which an individual's communications may be intercepted, the existence of a stringent authorization process for mass surveillance programs, a standardized method of choosing, analyzing, and using intercepted data, proper procedures to protect sensitive information and avoid illegal access or exposure when transmitting the intercepted material with third parties, the limits on the time duration of interception activities and the storage of intercepted material, the presence of a reliable impartial judicial body to guarantee the observance of the established safeguards, and the existence of some *ex post facto* mechanisms for independently

reviewing the compliance of the investigative operations with the interception safeguards.

The aforementioned new established eight safeguards brought the Grand Chamber to develop conclusions which not only will reflect on the countries at the center of the two distinct cases at stake, but they will permit other Council of Europe's adherent countries as well to commit perpetual violations of the Convention's fundamental rights.

In the light of this, throughout the third chapter judge Pinto de Albuquerque's concurring and dissenting opinion, member of the Grand Chamber of the ECtHR which delivered the final judgment, has been widely analyzed. The judge's opinion, harshly critical of that of his colleagues, is in a vein of little courage in this matter. Indeed, in his long contribution to the ruling the judge emphasized all the wrongdoing of his colleagues in delivering an obviously security-oriented decision. According to him, the work of the Court should have been citizen-oriented and not vice-versa. Mindful of this firm idea he managed to re-analyze the facts with a different point of view.

In sum, the judge deconstructed the final decision and re-elaborated the eight safeguards previously established by the Grand Chamber with the firm belief that the ECtHR's Grand Chamber's ruling not only could have eroded the Court's authority but also could have lessened the significance of the judgment as a benchmark for future cases, allowing the responding states to use its own discretion in enforcing the ruling.

Throughout de Albuquerque's opinion delivered in *Big Brother Watch*, which must be read parallelly to the statement he delivered at the end of the *Centrum För Rättvisa* final decision paper, the judge touched some aspects that the Grand Chamber barely considered during the years it dedicated to the cases at stake: one above all is undoubtedly the possibility for an extraterritorial application of the rights enshrined within the European Convention of Human Rights. Following the judge's grievances over this shortcoming, it has been decided to make a digression of the concept trying to understand why the judge found was disconcerted by this lack of the Court.

As demonstrated in the section on the principle of extraterritoriality, on several occasions during the last decades, the Court already had dealt with the question of extraterritoriality managing to develop a quite deep legal framework. Consequently, there is no clear explanation as to why the Court has decided not to deal with such a

complex issue, all the more reason in cases concerning the bulk interception of private data operated, in the majority of the cases, outside the boundaries of the countries at the center of the lawsuits: suffice it to consider that throughout the entire 204 pages of the final decision's paper of *Big Brother Watch* the expression "*extraterritoriality*" could be identified just once and only within the concurring words of judge de Albuquerque: this may lead to believe that the Court may have been too light in directing the final judgement.

The European Court of Human Rights has long been considered a guardian of fundamental human rights in Europe. However, recent decisions taken by the Council of Europe's highest judicial body regarding article 8 of the ECHR have prompted scholars to question whether the Court's focus has shifted towards security interests at the expense of individual liberties. From the analysis made throughout the thesis, with particular reference to the three landmark cases of the ECtHR of *Zakharov*, *Big Brother Watch*, and *Centrum För Rättvisa*, the answers to the interrogatives which drove the entire work should be clear: by considering frequent bulk interception operations as helpful, the Court has gradually begun to consider them as a fundamental tool in the hands of secret service agencies. Rather digging deep to find a correct balance between the security needs of a given country and citizens' privacy rights, it seems that the Court confined itself to accepting the new intrusive techniques as a *fait accompli*. It appears that within the Court's walls, the expression "usefulness" is gradually substituting the word "proportionality". It is crystal-clear that the world has changed after the 9/11 events, especially in terms of security, but this should not serve as a justification for the most important Council of Europe's judicial body to radically change the purpose of his work, that is to say protecting individuals from violations of their fundamental rights.

The new direction the Court seems to have taken in terms of privacy rights is nebulous and its implications on the broader landscape of human rights in Europe should not be disregarded. Balancing security and individual rights will remain a challenging task and it will be crucial for the ECtHR to retrun to a principled and balanced approach that safeguards both aspects of the European Convention on Human Rights effectively. Quoting judge Pinto de Albuquerque, "For good or ill, and I believe for ill more than for good, with the present judgment the Strasbourg Court has just opened the gates for an electronic "Big Brother" in Europe. If this is the new normal

that my learned colleagues in the majority want for Europe, I cannot join them, and this I say with a disenchanted heart, with the same consternation as that exuding from Gregorio Allegri's Miserere mei, Deus".

REFERENCES

Arnbak A. & Goldberg, S., *Loopholes for Circumventing the Constitution: Unrestricted Bulk Surveillance on Americans by Collecting Network Traffic Abroad* in *Michigan Telecommunications and Technology Law Review*, 2015, 21(2), 317-362.

Bauman Z., Bigo D., Esteves P., Guild E., Jabri V., Lyon D. & Walker R. B. J., *After Snowden: Rethinking the Impact of Surveillance* in *International Political Sociology*, 2014, 8(2), 121–144.

Bergen P., Sterman D., Schneider E., & Cahall B., *Do NSA's Bulk Surveillance Programs Stop Terrorists?*, New America, 2014.

Calmes J., Obama Says Surveillance Helped in Case in Germany, 2013 [Online], Available at: https://www.nytimes.com/2013/06/20/world/europe/obama-in-germany.html.

Case of *Big Brother Watch and Others v. The United Kingdom*, Judgment of the European Court of Human Rights, 2021.

Case of *Centrum För Rättvisa v. Sweden*, Judgment of the European Court of Human Rights, 2021.

Case of *Digital Rights Ireland Ltd v. Minister for Communication et al and Kärtner Landesregierung*, Judgment of the European Court of Justice, 2014.

Case of *Zakharov v. Russia*, Judgment of the European Court of Human Rights, 2015.

Congressional Record, House of Representatives, 113th Cong., 2013.

Custers B., Sears A. M., Dechesne F., Georgieva I., Tani T. & van der Hof S., *EU Personal Data Protection in Policy and Practice* in *Information Technology and Law Series*, 2019.

Diggelmann O. & Cleis, M. N., *How the Right to Privacy Became a Human Right* in *Human Rights Law Review*, 2014, 14(3), 441–458.

Disclosure of National Security Agency Surveillance Programs: Hearing before the H. Perm. Select Comm. on Intelligence, 113th Cong., statement of Gen. Keith Alexander, Director of NSA, 2013.

European Commission for Democracy Through Law (Venice Commission), *Report on the Democratic Oversight of Signals Intelligence Agencies*, Strasbourg, 15 December 2015.

Fabbrini F., *The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court*, Forthcoming in Sybe de Vries (ed.), *Five years of Legally Binding Charter of Fundamental Rights* in *iCourts Working Paper Series,* 2015, 19.

Frigo M., *Big Brother Watch v. UK: A Landmark Judgment Missing the Mark*, International Commission of Jurists, 4 June 2021 [Online], Available at: https://www.icj.org/big-brother-watch-v-uk-a-landmark-judgment-missing-the-mark/.

Georgieva I., *The Right to Privacy Under Fire Foreign Surveillance Under the NSA and the GCHQ and its Compatibility With art. 17 ICCPR and art. ECHR* in *Utrecht Journal of International and European Law*, 2015, 31(80), 104-130.

Goldsmith J., *Three Years Later: How Snowden Helped the U.S. Intelligence Community* in Lawfare Blog, 2016 [Online], Available at: https://www.lawfareblog.com/three-years-later-how-snowden-helped-us-intelligence-community.

Gondek M., *Extraterritorial Application of The European Convention on Human Rights: Territorial Focus in the Age of Globalization?*, in *NILR*, 2005, 52(3).

Greenwald G., *Edward Snowden: the whistleblower behind the NSA surveillance revelations*, 2013 [Online], Available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Greenwald G., *NSA collecting phone records of millions of Verizon customers daily*, 2013 [Online], Available at: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Gutteridge H. H., *The comparative law of the right to privacy* in *Law Quarterly Review*, 1931, 47(2), 203-218.

Houston T., *Mass Surveillance and Terrorism: Does PRISM Keep Americans Safer?*, University of Tennessee, 2017.

Inkster N., *The Snowden revelations: Myths and misapprehensions* in *Survival Global Politics and Strategy*, 2014, 56(1), 51-60.

Karakaş I. and Bakırcı H., *Extraterritorial Application of the European Convention on Human Rights: Evolution of the Court's Jurisprudence on the Notions of Extraterritorial Jurisdiction and State Responsibility*, in A. van Aaken, I. Motoc (eds.), *The European Convention on Human Rights and General International Law,* Oxford, 2018, ch. VI.

Kovalenko Y., *The Right to Privacy and Protection of Personal Data: Emerging Trends and Implications for Development in Jurisprudence of European Court of Human Rights* in *Masaryk University Journal of Law and Technology*, 2022, 16(1), 37–58.

Lawson R., *Life After Bankovic: On the Extraterritorial Application of the European Convention on Human Rights* in Coomans F. and Kamminga M. (eds), *Extraterritorial Application of Human Rights,* Intersentia, 2004, 83-123.

Lehman J. A.,*The right to privacy in Germany* in *New York University Journal of International Law and Politics*, 1968, 1(1), 106-127.

Lin H., *Having a conversation about bulk surveillance* in *Communications of the ACM*, 2016, 59(2), 40–42.

Lubin A., *Introductory Note to Big Brother Watch v. UK (Eur. Ct. H.R. Grand Chamber),* in *International Legal Materials*, 2022, 61(4).

Lubin A., *Legitimizing Foreign Mass Surveillance in the European Court of Human Rights* in *Just Security*, 2 August 2018.

Lyon D., *Surveillance, Snowden, and Big Data: Capacities, consequences, critique* in *Big Data & Society*, 2014, 1(2).

MacAskill E., “No regrets”, says Edward Snowden, after 10 years in exile, 2023 [Online], Available at: https://www.theguardian.com/us-news/2023/jun/08/no-regrets-says-edward-snowden-after-10-years-in-exile.

Mance J., *Human Rights, Privacy and the Public Interest—Who Draws the Line and Where?* In *Liverpool Law Review*, 2009, 30(3), 263–283.

Rojszczak, M., *The ECTHR’s judgment in the case of Centrum för Rättvisa v. Sweden as a leading case for the review of domestic regulations on signals surveillance* in *Problemy Współczesnego Prawa Międzynarodowego, Europejskiego I Porównawczego*, 2019, 17, 84–103.

Milaj, J., *Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance* in *International Review of Law, Computers & Technology*, 2015, 30(3), 115–130.

Milanovic M., *ECtHR Judgment in Big Brother Watch v. UK*, in *Ejiltalk*, 17 September 2018.

Miller S., *Revisiting Extraterritorial Jurisdiction: A Territorial Justification for Extraterritorial Jurisdiction under the European Convention* in *The European Journal of International Law*, 2009, 20(4), 1223–26.

Murray D. & Fussey P., *Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data* in *Israel Law Review*, 2019, 52(1), 31-60.

Pohle J. & Audenhove L. V., *Post-Snowden Internet Policy: Between Public Outrage, Resistance and Policy Change* in *Media and Communication*, 2017, 5(1), 1-6.

Reddick C. G., Chatfield A. T. & Jaramillo, P. A., *Public opinion on National Security Agency surveillance programs: A multi-method approach* in *Government Information Quarterly*, 2015, 32(2), 129-141.

Reid A. S. & Ryder N., *For Whose Eyes Only? A Critique of the United Kingdom’s Regulation of Investigatory Powers Act 2000* in *Information & Communications Technology Law*, 2001, 10(2), 179–201.

Sajfert J., *The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights,* in *EuLawBlog*, 8 June 2021.

Sawyer, S., *Government Bulk Surveillance from 1978-2020: an Ongoing Violation of Citizens Rights*, 2020, Doctoral dissertation, Syracuse University.

Scheuerman W. E., *Whistleblowing as civil disobedience: The case of Edward Snowden* in *Philosophy & Social Criticism*, 2014, 40(7), 609-628.

Stanley J. E., *Max mosley and the english right to privacy* in *Washington University Global Studies Law Review*, 2011, 10(3), 641-668.

Tiberi G., *Il caso Big Brother Watch quale cambio di paradigma nel bilanciamento tra sicurezza e tutela dei diritti fondamentali?*, in *Quad. cost.*, 2018, 4.

Trouille H., *Private Life and Public Image: Privacy Legislation in France* In *International and Comparative Law Quarterly*, 2000, 49(1), 199–208.

Turanjanin V., *When does bulk interception of communications violate the right to privacy? The limits of the state's power and the European Court of Human Rights Approach* in *International Cybersecurity Law Review*, 2022, 4, 115-136.

van der Sloot B., *The quality of law: How the european court of human rights gradually became a european constitutional court for privacy cases*, in *J. Intell. Prop. Info. Tech. & Elec. Com. L. 160*, 2020, 11(2).

Vauchez, S. H., *The State of Emergency in France: Days Without End?* in *European Constitutional Law Review*, 2018, 14(4), 700–720.

Vogiatzoglou P., *Centrum for rattvisa v sweden: Bulk interception of communications by intelligence services in sweden does not violate the right to privacy*, in *Eur. Data Prot. L. Rev. 563*, 2018, 4(4).

Wagner, W. J., *The Development of the Theory of the Right to Privacy in France* in *Washington University Law Quarterly*, 1971, 1971(1), 45-72.

Warren S. D. & Brandeis L. D., *The Right to Privacy* in *Harvard Law Review*, 1890, 4(5), 193–220.

Watt E., *Much Ado About Mass Surveillance – the ECHR Grand Chamber 'Opens the Gates of an Electronic "Big Brother" in Europe' in Big Brother Watch v UK*, in *Strasobs*, 28 June 2021.

Woods L., *Zakharov v. Russia (Eur. Ct. H.R.)* in *International Legal Materials*, 2016, 55(2), 207-266.

Yoo J., *The legality of the national security agency's bulk data surveillance programs* in *Harvard Journal of Law & Public Policy*, 2014, 37(3), 901-930.

Zalnieriute M., *Big Brother Watch and Others v. the United Kingdom*, in *American Journal of International Law*, 2022, 116(3).

Zalnieriute M., *Big Brother Watch v. UK*, in *VerfBlog*, 2 June 2021.

EXCECUTIVE SUMMARY

With the beginning of the 21st century, the European Court of Human Rights found itself burdened with a myriad of cases regarding the right to privacy, with possible violations of article 8 of the European Convention of Human Rights. The origin of this new direction of the ECtHR gradually becoming a European Constitutional Court for privacy rights could be identified in the 9/11 terrorist attacks. The unprecedented massacres unveiled a totally inappropriate security system, not only in the United States of America, but in the other powerful countries too. The secret surveillance measures adopted until then were not sufficient anymore to prevent dormant threats to undermine the stability of the established order. In this context new, technological, and most of all, intrusive surveillance programs, were enacted all over the world without the acknowledgment of the citizens: mass surveillance and bulk interception methods expanded surveillance powers in the hands of intelligent agencies creating serious implications concerning human rights protection, particularly with the right to privacy.

The debate on privacy and security necessities revolves around proportionality, consent, accountability, and the balance between secrecy and transparency. The first aforementioned principle, proportionality, allows for the protection of the right to privacy while justifying its limitation in certain situations. Surveillance practices often go without citizens' knowledge or consent, making it difficult to notify thousands of citizens simultaneously. Accountability is crucial, as secret services require protection of sensitive information and operational details. However, little oversight can lead to abuses of power, violations of fundamental rights, and operations outside the law. To balance these concerns, an independent, non-political body should be entrusted with monitoring intelligence agencies to ensure they operate within the law.

To understand the complex framework which has been built around the right to privacy in Europe over the last two decades, it is essential to analyze the right's regulation at a national and at a European level, examine the Charter of Fundamental Rights of the European Union with its main articles regulating privacy needs of the European citizens to be found in articles 7 and 8, and consider the European Court of Human Rights' perspective on privacy with the unprecedented 2015 decision of *Roman Zakharov v. Russia* which set a European standard for future judgments as the pivotal case of *Big Brother Watch and Others v. the United Kingdom*, concerning privacy.

The right to privacy in Europe has a complex legal framework, with each country having its own laws and regulations. Regional organizations also establish guidelines to ensure uniform protection across European borders. Italy, France, Germany and the United Kingdom are four national examples of regional legislations brought in the first chapter.

Italy has a strong legal framework concerning the right to privacy, including constitutional provisions, national laws, and regulations. It is bound by all EU legislation, with most national laws and provisions enacted to standardize Italy to the European standard set in various European Directives and Regulations ordered by the European Union.

The constitutionally protected side of the right to privacy includes articles 13 to 28, with particular reference to articles 14 and 15, which emphasize the inviolability of people's home and personal domicile and grants the safeguard and secrecy of each form of communication, starting from written correspondence. Limitations to these rights can be made only by judicial bodies which must state the reasons behind the limitation, and in accordance with the guarantees established by Italian law.

Italy has several laws protecting privacy, most of which were established to comply with European Regulations and Directives. Law 675 of December 1996 established the Italian Data Protection Authority (IDPA) to protect people and other subjects concerning the treatment of personal data. The Personal Data Protection Code (PDPC) was introduced to unify the data protection framework and introduced conduct guidelines for journalistic, historical, scientific, or statistical activities.

France has a monistic approach towards international law, with no requirement for international treaties to be incorporated into national legislation. The protection of the right to privacy in France is a perfect mixture between national provisions and European regulations. The main provision for privacy in France is the July 1970 Act of Parliament, which modified both the Criminal and Civil Codes. This law defines a new framework concerning possible violations or offenses to the privacy of citizens and the consequent sanctions.

Personal data protection in France is regulated mostly through sectoral provisions, such as online electronic communication services, consumer rights to privacy, the Public Health Code, and the Property Code. As a member of the European Union,

France has its own interpretation of the European General Data Protection Regulation, the French Data Protection Act which poses fundamental obligations to individuals and organizations, including processing personal data with relevant legal and financial reasons, providing clear information about privacy policies, and obtaining explicit consent for processing private data.

France has an independent body, the Commission Nationale de l'Informatique et des Libertés (CNIL), which was strengthened by the European GDPR in 2018 to apply European Parliament will. Nowadays, the CNIL has stronger investigation means and the ability to elaborate "soft laws" such as guidelines, recommendations, and standards to be followed by French individuals or collectives.

Right to privacy in Germany has a complex legal framework too, with both federal and state governments having the authority to pass laws and oversee compliance with the European Directives. The German Basic Law outlines specific areas of responsibility exclusively held by the federation, while all other responsibilities remain under the jurisdiction of individual states.

The EU Data Protection Directive 95/46/EC placed the first fundamental dowel for the right to privacy protection in Europe, and 16 states of the German federation anticipated German federal legislators in implementing the Directive. The 1995 European Directive was the first deep modification to the European right to privacy legal landscape, and in 2001, an official federal legislation came into force. Two amendments were passed in 2003 and 2009, mainly aimed at regulating the duties of privacy officers and facilitating judges in cases concerning private data. The more recent Bundesdatenschultzgesetz (FDPA) was designed to apply the decisions of the GDPR to the German country, creating a Federal Commissioner for Data Protection and Freedom of Information to check on data protection in public offices, corporations, and telecommunication and postal services.

Finally, in the United Kingdom, the protection of the right to privacy is at least peculiar. The 1998 Human Rights Act allowed for easy incorporation of internationally recognized principles, including the right to privacy, into the British domestic legal system. English courts faced several cases concerning the new signed Human Rights Act, leading to the development of a stronger legal base concerning the right to privacy even in a country based on a Common Law model.

The right to privacy within the European Union legal framework has been a significant issue for European lawmakers since the 1990s. Directives and Regulations, such as Directive 96/46 and the 2016 General Data Protection Regulation (GDPR), have allowed for regulation of privacy rights. The European Charter of Fundamental Rights, signed in 2000, is the primary source of law for protecting individual rights and freedoms within the EU. Articles 7 and 8 of the Charter of Fundamental Rights make direct reference to the right to privacy, with Article 7 focusing on the private life of individuals and Article 8 on the protection of personal data.

The *Digital Rights Ireland Ltd v. Minister for Communication* case was a pivotal decision in the EU' efforts to protect privacy rights. The European Court of Justice (ECJ) took a peculiar approach, invalidating an entire piece of EU legislation, a Directive dated 2006, for a violation of articles 7 and 8 of the aforementioned Charter. The 2006 Directive, which was a direct consequence of the Madrid massacres of the same year, laid down the obligation on providers of publicly available electronic communications services or networks to retain telecommunication data necessary to identify source, destination, date, time, duration of a communication, the equipment with which the user sent the communication, and their location. The Directive provided security authorities with a powerful tool to investigate and reprimand crimes, but also significantly impacted the right to privacy.

The European Data Retention Directive faced opposition from Ireland, which argued it violated fundamental rights, including the right to privacy and protection of personal data. The Irish Constitutional Courts challenged the Directive, arguing it violated principles of necessity and proportionality, interfered with freedom of expression and association, and lacked harmonization in implementing it across member states. The European Court of Justice found that the Directive should have at least respected three main criterions: not overcoming the essence of the rights listed in articles 7 and 8, meeting an objective of general interest, and being strictly necessary to reach that objective by correctly balancing between security and citizen privacy. The ECJ's opinion was against the Directive obligations in the fight against international terrorism, as it considered the retention of data beyond the crimes themselves.

Parallel to the ECJ, the European Court of Human Rights works under the European Convention of Human Rights. Article 8 of the ECHR is the most known guarantee

against any kind of abuse of citizens' private life. It primarily serves as a right aimed at countering interferences by the State. The second paragraph of the article refers to the justifications for legally permitted interferences with the right to private and family life. The article requires that any interference must be authorized by domestic legislation and not arbitrary in nature. The expression of "*necessary to a democratic society*" underlined in the article, recognizes that interferences must pursue a legitimate aim, be proportionate, and respect the core values and principles of democracy. The standards set in the aftermath of *Zakharov v. Russia* were based on these principles.

The *Roman Zakharov v. Russia* case marked a significant turning point in the legal framework surrounding the right to privacy in Europe: indeed, the 2015 decision, which influenced the *Big Brother Watch and Others v. the United Kingdom* case, set standards that may change the ECtHR's approach towards national security interests at the expense of citizens' privacy. The case involved Roman Andreyevich Zakharov, a publishing company editor and chairperson of the St. Petersburg branch of the Glasnost Defense Foundation. Zakharov claimed that the Russian Ministry of Communications' Order 70 violated his private life. The ECtHR accepted Zakharov's application based on the recognition of the influence of the legislation on every user of communication, regardless of proof of direct surveillance.

The European Court of Human Rights has ruled that any law limiting the scope of the right to privacy must be done in accordance with the law, in the interests of national security, public safety, or economic well-being of a country, and necessary to a democratic society. The Court analyzed the wording "*in accordance with the law*" and its intrinsic meaning, stating that domestic law must meet quality requirements, be accessible to individuals, and foreseeable in its effects. The Court established the "Weber criteria", six standards that any law limiting the scope of the right to privacy must respect. The criteria included the nature of the offenses that may give rise to an interception of private data order, the procedure for collecting, storing, and analyzing data, and the precautions taken by secret services when sending private information to third parties. The Court emphasized that if even only one of the criteria had not been respected, it would not have allowed any law to be passed by the national legislators.

The Strasbourg Court ruled that Russian legal provisions governing interceptions of communications did not provide adequate guarantees against arbitrariness and the risk

of abuse inherent in any system of secret surveillance. The Court emphasized the need for clear rules governing the scope and implementation of surveillance measures and effective oversight mechanisms to prevent abuse.

The *Zakharov* case has had a notable influence on how privacy rights and surveillance practices will be understood throughout Europe. It strengthened the need for sufficient safeguards, oversight, and remedies in relation to government surveillance activities, but also set the basis for the controversial decision of *Big Brother Watch and Others v. the United Kingdom*. The judgment also played a part in ongoing discussions about finding the right balance between national security and individual privacy, along with the necessity for strong legal frameworks to govern surveillance in the digital era.

Before dealing with the *Big Brother Watch* ruling, the events which generated the lawsuit should be closely analyzed. Edward Snowden exposed the world's secret surveillance system during the first decade of the 20th century, highlighting the moral and concrete harm of bulk interceptions.

Bulk interceptions are the new crucial tool for intelligence agencies to collect vast amounts of communications data, enabling the identification of emerging threats and terrorist activities. However, this approach raises concerns about privacy and data protection, as the vast amount of data collected can lead to a culture of mass surveillance and eroding individual privacy rights. The sheer volume of data collected through bulk interceptions encompasses communications of countless individuals who are not suspected of any wrongdoing, possibly making the act unnecessary for a democratic society. Privacy implications are compounded by the storage and retention of this data for extended periods, allowing for future analysis or potential misuse. The use of advanced technologies for automated data processing and analysis poses additional privacy challenges, as the reliance on algorithms and machine learning techniques raises concerns about accuracy and potential bias in identifying threats. Balancing the need for effective security measures with the preservation of privacy rights is a complex task that requires robust legal frameworks, comprehensive oversight mechanisms, and transparent accountability measures. The European Court of Human Rights was already working towards a well-balanced legal framework, but the Snowden revelations opened Pandora's box, revealing how intrusive were the investigative operations conducted by

some of the most powerful secret services including the North American NSA and the British GCHQ.

The 2001 USA Patriot Act, also known as the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act", was at the basis of Snowden's decision to reveal to the world the existence of such invasive investigation programs: three main sections of the Act, Section 206, Section 207, and Section 215, were crucial in understanding Edward Snowden's actions. Section 206 expanded the government's authority to conduct surveillance on individuals attempting to evade detection by frequently changing communication devices. Section 207 extended the maximum time allowed for FISA surveillance of non-U.S. persons, allowing investigators to gather intelligence on potential threats and streamline the surveillance process. Section 215, the most debated, granted the government the authority to request access to business records without demonstrating probable cause or notifying the individual involved. This provision faced significant controversy due to potential infringements on privacy rights and First Amendment freedoms. Under the protection of the Patriot Act, agencies like the NSA and CIA continued to operate for years in search of possible terrorist plots against the United States.

Edward Snowden's revelations exposed the extent of global surveillance operations, including the Prism and Tempora programs. The data intercepted under Tempora, a UK Government Communications Headquarters program, was massive and directed to GCHQ's monitoring stations, where it was stored using the agency's Internet buffers. The data was then searched using keywords agreed upon by both GCHQ and the NSA, totaling approximately 40,000 selector pointers.

As it can be easily witnessed, Snowden's revelations did not only focus on the United States intelligence agencies but also on operations carried out by its allies, that is to say the British GCHQ and the "Five Eyes". Both the NSA and GCHQ mutually benefited each other, with a significant portion of data obtained through the PRISM program transferred to GCHQ servers. Tempora also contributed to the NSA's work, allowing the American agency to have a wider control over potential threats.

The revelations led to several scenarios, including the need for major powers to explain their secret surveillance programs to citizens and determine if they served their

purpose. Governments had to rebuild their intelligence networks to comply with people's needs of transparency and accountability. The legal framework concerning the right to privacy had to be renewed in the context of an ever more interconnected and technological world.

The whistleblower's actions provoked serious consequences as Snowden showed that the right to privacy was not respected concretely. European lawmakers were already working towards an upgrade of the legal landscape of this right, with the *Zahkarov v. Russia* case highlighting efforts from the European Court of Human Rights to find a balance between the right to privacy and increasingly technological methods of collecting and analyzing private data, but the former CIA contractor's revelations paved the way for the pivotal sentence of *Big Brother Watch and Others v. the United Kingdom*.

According to the Strasbourg Court, the European Convention on Human Rights' Article 8 is not always violated when communications are intercepted by using bulk interception means. The Court stressed the significance of complying to safeguards and oversight to prevent infringing people's Article 8 rights to privacy. The Grand Chamber further determined that the concepts of "*reasonable suspicion*" and "*subsequent notification*" do not apply to mass interceptions since the *Zakharov* case required different standards than the *Big Brother Watch* one.

In fact, the Court made a distinction between bulk interception and targeted surveillance, noting that the latter is more frequently utilized for acquiring foreign intelligence, early cyberattack identification and investigation, counterespionage, and counterterrorism. In addition, the Court adapted the Weber criteria from *Zakharov v. Russia* to the new bulk interception techniques, in some ways lowering them to recent technology advancements. The Court's focus was not on changing the legal climate of bulk interception regimes, but on the specific methods, requirements, and assurances outlined by national laws during the practical execution of these policies: the Court introduced eight comprehensive safeguards to ensure the protection of the privacy of the citizens, indeed making it easier for intelligence agencies to adapt their investigative techniques to the new established criteria.

Briefly analyzing the merits of the case, the ECtHR ruled that the UK's bulk interception regime violated privacy rights. The Court emphasized the need for clear

grounds for authorization, a robust authorization procedure, clear procedures for data collection, precautions when sharing intercepted material, and limits on interception activities and storage. The Court also highlighted the need for independent oversight and independent ex post facto review of compliance. The Grand Chamber found that the surveillance programs were not "*in accordance with the law*" and violated Article 8 of the European Convention on Human Rights. The sentence pushed privacy advocates to argue that the Court's decision may set a precedent for intrusive surveillance practices without adequate safeguards, potentially erasing privacy rights for individuals in the UK and across Europe.

The ruling in the Big Brother Watch case brought indeed to a lasting establishment of mass surveillance as a standard practice for many years ahead. Five justices who ruled the case were of the same opinion and, with several concurring and dissenting opinions, they tried to deliver an alternative opinion to the ruling. Judges Lemmens, Vehabović, Bošnjak, and Ranzoni found that the judgment missed a valuable opportunity to fully support the importance of privacy and correspondence in the face of intrusions such as mass surveillance. They argued that the majority had not adequately emphasized the importance of private life and correspondence when dealing with bulk interception. The judges also criticized the bulk interceptions phases: previously, the Grand Chamber had identified four stages in the bulk interception process where the level of intrusion in the citizens' life increased as the various phases progressed. The four judges stated that, contrary to the opinion of the majority, which considered only the final phases as the real intrusive moments of the processing of the collected data, the initial stage of investigation should have been considered an indispensable prerequisite for any subsequent stages of analysis, and should therefore be considered intrusive in itself.

The eight new safeguards established by the Grand Chamber have been harshly criticized, arguing that they did not function as independent minimum standards, lacked explicit substantive protection for individuals against excessive interference, and lacked procedural protection. The judges also highlighted a lack of clarity and transparency in the UK's interests of national security, potentially leading to misuse of interception methods.

Judge Pinto De Albuquerque criticized the Court's vague language, methodology, and the new established safeguards, arguing that those deficiencies could lead to inconsistent application across different cases and jurisdictions, weakening the Court's impact on human rights protection.

The dissenting judge denounced the European Court of Justice for abandoning the previous case law set in the *Zakharov v. Russia* case and for establishing a misleading, pro-security precedent in the European jurisprudence. In consequence he delivered a new citizen-oriented judgment, introducing a deeper and more complex list of safeguards to avoid potential violations of the right to privacy in Article 8 of the Convention.

As he criticized the absence of specific rules for professionals, the judge introduced a new principle to protect privileged professional communications, aiming to establish a specific protective regime for these professions. He emphasized the need for court authorization before intercepting communications originating or received by these professionals, and forbidding spying on communications governed by religious secrecy. The judge also blamed the majority's lack of consideration for receiving states' safeguards and the lack of clarity on the extent to which states can decide when to strengthen control over citizens.

There is one fundamental aspect which was not considered by the majority during the ruling of *Big Brother Watch and Others v. the United Kingdom* which left Judge Pinto de Albuquerque and the public opinion dissatisfied by the decision taken by the Grand Chamber of the ECtHR: the principle of extraterritoriality, that is to say the possibility for the European Convention of Human Rights to be applied outside the boarders of the European Union. It is not clear why the Court did not analyze this fundamental aspect while dealing with the merits of a case regarding mass surveillance when, during the last two decades, it worked towards an expansion of the aforementioned principle.

In the past, the Court has indeed faced some complexities in interpreting Article 1 of the ECHR, which places responsibilities of effective governance on Contracting States concerning individuals within their territory: in the *Banković and Others v. Belgium and 16 Other Contracting States* case of 2001, the Court pronounced against the application of the Convention outside the territorial limit of the contracting states

of the ECHR, but it still managed to develop some exceptions to what was emphasized in the first article of the Convention. These exceptions, as recognized by the Court could arise in cases of extradition or expulsion, extraterritorial effects, effective control, and consular or diplomatic cases. The Court has also recognized flag jurisdiction cases as possible situation of application of the Convention outside the EU boarders.

The principle of extraterritoriality has been furtherly developed in subsequent rulings throughout the 21st century. In 1995, the Court ruled that Turkey did not have jurisdiction over six shepherds killed in northern Iraq due to Turkish army military activities according to a strict lecture of Article 1 of the Convention in the case of *Issa and Others v. Turkey*. However, the Court argued that if it had been proven that the Turkish army forces were, even briefly, in effective control of the area in question, the shepherds would logically be under Turkish jurisdiction rather than Iraq's, which is not a Contracting State and is outside the legal space of the Contracting States. The *Öcalan v. Turkey* judgment expanded again the principle of extraterritorial application of the Convention: this time the Court made direct reference to ad hoc police operations in a foreign country by using the "*effective control*" principle. Departing from *Banković* the 2011 *Al-Skeini and Others v the United Kingdom* sentence marked a turning point in the legal framework of the principle, as it confirmed that contracting states must uphold their human rights obligations wherever their agents exercise authority and control over individuals. The *Jaloud v. The Netherlands* decision established that the mere practice of exercising authority over a checkpoint is sufficient to establish the jurisdiction of a contracting state outside the European Union boundaries.

To conclude the analysis of the *Big Brother Watch* sentence, the parallel decision of *Centrum För Rättvisa v. Sweden* must be briefly analyzed in order to have a thorough understanding of the legal basis for the right to privacy recently established by the ECtHR as the two rulings should not be read independently.

The non-governmental Swedish organization Centrum För Rättvisa filed a lawsuit challenging Swedish domestic legislation allowing secret surveillance regimes based on signals intelligence, which it argued violated Article 8 of the European Convention of Human Rights. The organization criticized the powers of the National Defense Radio Establishment, a branch of the Swedish Ministry of Defense, under the 2000 Act on Foreign Intelligence and Regulation of the Minister of Defense on Signals Intelligence

and the 2008 Act on Signals Intelligence. The European Court of Human Rights found the Swedish legislation regulating mass surveillance practices in accordance with the Convention, with no violation of the right to privacy. The Grand Chamber overturned the First Section's Chamber decision, focusing on the domestic law's adequate and effective safeguards and guarantees to meet the requirements of foreseeability and necessity in a democratic society. The Court found that the Swedish Act of Signals Intelligence relied on adequate legal standards, provided clear grounds for surveillance authorizations, correctly regulated the duration of an interception, and adequately monitored the procedures for collecting and analyzing intercepted data, but it identified three main deficiencies which made the legislation violating article 8 of the Convention: first, there was no clear policy on how to deal with intercepted data that is not personal information; second, there was no requirement to take into account people's privacy concerns when providing information to foreign intelligence agencies; and third, there was no effective retrospective review procedure..

As in the *Big Brother Watch* decision, Judge Pinto de Albuquerque issued a concurring opinion attached to the Strasbourg Court's final decision on the Swedish government's intelligence practices. Substantially, he reiterated what he already well made explicit during the parallel ruling: he argued that the Court's biased methodology and vague language led to a defective regime, expressing concern over a potential electronic "Big Brother" in Europe.

In conclusion, as it has been tried to demonstrate throughout the work, the recent landmark decisions of the Strasbourg Court have opened the gate for an electronic "Big Brother" in Europe. Judge de Albuquerque concerns over the future of the right to privacy in Europe are at least shareable due to the recent rulings of the Court which can be considered too light in terms of balancing security needs and privacy rights. The ECtHR's work should be, on the contrary, driven by a meticulous analysis and most of all proportionality-oriented: hopes are that in the judgments to come, the Court will review its jurisprudence with the objective of returning to a principled and balanced approach, thus seeking to protect fundamental human rights while also respecting the need for greater security against the threats brought by the 21st century.